Gegevensbeschermings-effectbeoordeling (DPIA)

Windows 10 Enterprise Eindrapport

Privacy Management Partners

Utrecht, 11 juni 2018

in opdracht van het Ministerie van Justitie en Veiligheid ten behoeve van SLM rijk

Gegevensbeschermings-effectbeoordeling (PIA)

Windows 10 Enterprise

Eindrapport

Privacy Management Partners

in opdracht van het Ministerie van Justitie en Veiligheid

ten behoeve van SLM rijk

Opdrachtgever:	Ministerie van Justitie en Veiligheid (JenV) ten behoeve van SLM Rijk Directie Infomatievoorziening en Inkoop (DI&I)
Auteurs:	dr. Koen Versmissen CIPP/E CIPM CIPT FIP Jacques Eding MSc RE CIPP/E CIPM CIPT FIP CISSP CISM mr.drs. Jeroen Terstegge CIPP/E
Versie:	eindrapport, versie 1.1 van 11 juni 2018
	Voor vragen en opmerkingen over deze DPIA kunt u terecht bij: P. van den Berg, Strategisch Leveranciers Management Microsoft Rijk DI&I

Inhoudsopgave

Managementsamenvatting

In opdracht van de Directie Informatievoorziening en Inkoop (DI&I) van het Ministerie van Justitie en Veiligheid heeft Privacy Management Partners een gegevensbeschermingseffectbeoordeling (Data Protection Impact Assessment, DPIA) conform de Algemene Verordening voor Gegevensbescherming (AVG) uitgevoerd op het gebruik van telemetrie door (onderdelen van) Microsoft in Ierland dan wel Amerika. Telemetrie is het stelselmatig verzamelen en verwerken van gegevens over het gebruik van software en het functioneren van het apparaat waarop deze software is geïnstalleerd. Bij de toepassing van telemetrie door Microsoft kunnen persoonsgegevens verwerkt worden waarmee de AVG van toepassing is. Op grond van de AVG dient een DPIA te worden gehanteerd wanneer verwerkingen risico's kunnen inhouden voor de privacyrechten van betrokkenen. De directe aanleiding voor de DPIA was de uitkomst van een onderzoek door de Autoriteit Persoonsgegevens (AP) naar telemetrie in Windows 10 Home en Pro. De AP constateerde daarin dat de gegevensverwerking op diverse essentiële aspecten de gegevensbeschermingswetgeving overtrad. Om risico's bij het gebruik van Microsoft enterprise producten zoveel mogelijk te voorkomen en te beperken is daarom over gegaan tot het uitvoeren van deze DPIA.

Conform het Model GEB Rijksdienst bestaat de DPIA uit de volgende onderdelen:

A. Feitelijke gegevensverwerking telemetrie;
B. Beoordeling van de rechtmatigheid;
C. Beschrijving en beoordeling van de risico's voor betrokkenen;
D. Beschrijving beheersmaatregelen

De DPIA richtte zich primair op de verwerking van persoonsgegevens bij het gebruik van telemetrie in het Microsoft-product Windows 10 Enterprise en op de verdere verwerking van deze gegevens. Naar zijn aard gaat deze DPIA vooral in op de risico's van telemetrie voor de rechten en vrijheden van betrokkenen. Naar aanleiding van de resultaten van de DPIA en in aanvulling hierop zullen ook de aspecten veiligheid en functionaliteit bij besluitvorming over de inzet van de software moeten worden gewogen.

Proces

Deze DPIA is niet in opdracht van alle betrokken verwerkingsverantwoordelijken opgesteld. Microsoft heeft laten weten als verwerkingsverantwoordelijke afzonderlijk een DPIA te zullen uitvoeren. Hiernaast heeft Microsoft gelegenheid gekregen bij te dragen aan onderdeel A van deze DPIA, de beschrijving van de feitelijke gegevensverwerkingen.

Het instrument van de DPIA is toegepast op een algemeen kader met betrekking tot de Microsoftproducten. Overheidsinstanties dienen, op basis van dit algemene kader, voor hun specifieke bedrijfsproces een DPIA op te stellen, doordat de mate van verantwoordelijkheid in de zin van de privacywetgeving uiteindelijk afhankelijk is van de feitelijke invloed die overheidsinstanties op verwerkingen hebben. Zo is dit onder meer afhankelijk van de instellingen van het niveau van telemetrie.

De DPIA is een dynamisch instrument, dit betekent dat wanneer het feitelijk of juridisch kader veranderd, dan wel er nieuwe inzichten ontstaan, deze DPIA zal worden herijkt en een nieuwe toetsing van de risico's voor de privacyrechten van betrokkenen zal worden uitgevoerd.

Voorlopige conclusie

De belangrijkste voorlopige conclusie van de DPIA is dat in beginsel een overheidsinstantie die kiest voor telemetrie op het niveau Security AVG-conform handelt. Een keuze voor een hoger niveau van telemetrie zou op basis van een specifieke belangenafweging nader onderbouwd moeten worden.

De conclusie dat telemetrie op niveau Security AVG-conform is, is nadrukkelijk gebaseerd op de slechts marginaal beoordeelde aanname dat Microsoft bij de verwerking van telemetriegegevens AVG-conform handelt, en op niet altijd volledige, consistente en te doorgronden informatie van Microsoft over die verwerking.

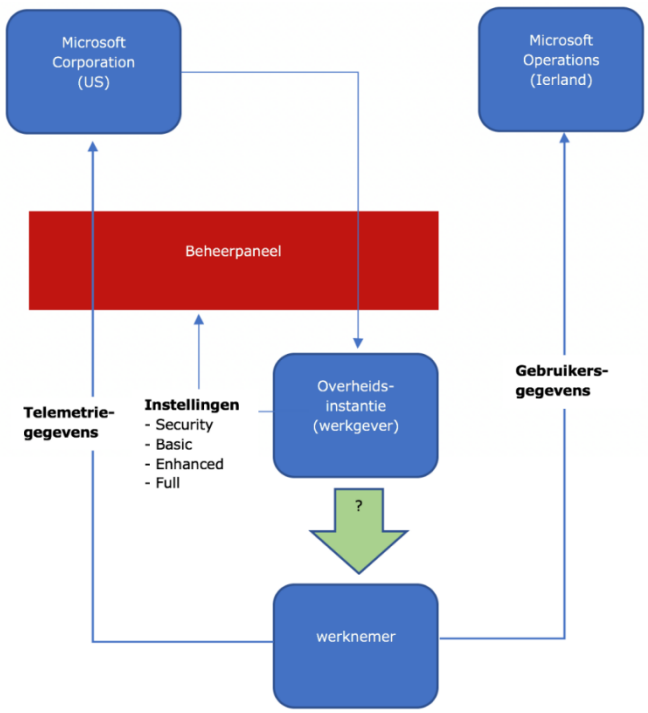
A. Feitelijke gegevensverwerking

Het eerste onderdeel van de DPIA betreft een beschrijving van de feitelijke verwerkingen die plaatsvinden bij het gebruik van Windows 10 Enterprise (versie 1803). Alle in het kader van telemetrie verwerkte gegevens zijn in beginsel te beschouwen als persoonsgegevens. Microsoft onderscheidt vijf niveaus van verwerking van deze gegevens. Op het laagste niveau, Security, verwerkt Microsoft alleen informatie die nodig is voor beveiligingsfunctionaliteit zoals Windows Defender en de Malicious Software Removal Tool. Op het een na laagste niveau, Basic, worden al een groot aantal aanvullende gegevens verwerkt die niet het belang van de klant of zijn werknemers dienen. Microsoft biedt ook een script aan waarmee de overdracht van telemetriegegevens volledig kan worden uitgeschakeld. Dat brengt echter wel een belangrijk verlies aan functionaliteit (op het gebied van beveiliging) met zich mee.

Telemetrie in Windows heeft als doel om Windows actueel, veilig en betrouwbaar te houden en goede prestaties te waarborgen; om Windows op basis van statistische analyses te verbeteren; en om gebruikersinterfaces te personaliseren. Het gebruik van telemetrie past in een transformatie van Microsoft van een leverancier van producten naar een dienstverlener (“Windows as a service”).

Rollen

Microsoft is de verwerkingsverantwoordelijke voor het gebruik van telemetriegegevens. Voor de overdracht van die gegevens naar Microsoft is de overheidsinstantie die van Windows gebruik maakt mede-verwerkingsverantwoordelijke voor zover zij invloed heeft op het doel en de middelen voor verwerking. Den overheidsinstantie kan namelijk het niveau van telemetrie bepalen, daarmee wordt essentiële invloed uitgeoefend op (de middelen van) de verwerking en is zij daarmee verwerkingsverantwoordelijke.



De overheidsinstantie moet meerdere (mogelijk tegengestelde) belangen tegen elkaar afwegen. Enerzijds dient zij zich te gedragen als goed werkgever, en moet zij haar werknemers dus niet blootstellen aan onnodige verwerking van hun persoonsgegevens. Anderzijds moet zij het haar werknemers ook mogelijk maken om veilig en gemakkelijk te werken; meer in het algemeen dient zij ook haar informatiebeveiliging op orde te. hebben.

B. Beoordeling rechtmatigheid

Op basis van de verkregen feiten zoals omschreven in onderdeel A heeft een beoordeling van de rechtsgrond, noodzaak en doelbinding plaatsgevonden. Of Microsoft een valide rechtsgrond heeft voor de verwerking van telemetriegegevens dient elke overheidsinstantie, onder meer op basis van de bestaande overeenkomsten met primair zelf te beoordelen. Klanten kunnen een marginale toets doen of Microsoft daarbij de juiste afwegingen maakt. Deze DPIA biedt daarvoor een eerste basis, zij het dat er nog veel zaken onduidelijk zijn gebleven.

Voor de overheidsinstantie is een keuze voor telemetrie op niveau Security goed te motiveren vanuit het oogpunt van met name beveiliging. Indien hogere niveaus van telemetrie worden gehanteerd worden er meer persoonsgegevens verwerkt waarmee de risico's voor betrokkenen wellicht onnodig worden verhoogd, want dit dient voornamelijk het belang van Microsoft. De aanbeveling aan overheidsinstanties is dan ook om te kiezen voor telemetrie op niveau Security.

Telemetrie valt onder de bepalingen van de Telecommunicatiewet (gebaseerd op de Europese e-Privacyrichtlijn) en de komende e-Privacyverordening over toegang tot informatie in de randapparatuur van een gebruiker. Deze wetten hebben als zogeheten 'lex specialis' voorrang op de bepalingen van de AVG. Hierover luiden de conclusies als volgt.

Onder de Telecommunicatiewet is telemetrie toegestaan indien en voor zover die strikt noodzakelijk is om een gevraagde dienst te leveren, of om informatie te krijgen over de kwaliteit of effectiviteit

van de geleverde dienst. In dat laatste geval moeten de privacygevolgen voor de werknemers klein of afwezig zijn.

Onder de huidige concepttekst van de e-Privacyverordening is telemetrie op basis van de huidige situatie niet toegestaan

C. Risico's voor betrokkenen

De kernconclusies als het gaat om de risico's voor de werknemers die met Microsoft-software werken, luiden als volgt.

- Telemetrie brengt risico's met zich mee voor de persoonlijke levenssfeer en de rechten en vrijheden van de betrokken werknemers.
- Die risico's zijn echter vanuit het oogpunt van de betrokkene beperkt in omvang. Dat is met name het geval omdat telemetrie (vrijwel) geen effecten beoogt voor de individuele eindgebruiker, en Microsoft (naar eigen zeggen) AVG-compliant werkt. Eventuele beveiligingsrisico's voor de overheidsinstantie door de hoeveelheid gegevens zijn niet meegewogen in deze DPIA. Hiervoor moet een separate veiligheidsinschatting worden gemaakt
- De mogelijke risico's kunnen verder beperkt worden door te kiezen voor het telemetrie niveau Security. De nadelige gevolgen daarvan qua functionaliteit zijn beperkt. Er kan ook gekozen worden voor een script waarbij alle telemetrie uitgezet kan worden. Hoewel het risico hiermee nog verder wordt beperkt zal dit script, zonder aanpassingen, ook essentiële functionaliteiten raken.

Kanttekeningen hierbij zijn dat het moeilijk is om zicht te krijgen op wat Microsoft precies doet, en er geen zekerheden zijn dat dit in de toekomst niet gaat veranderen. Deze DPIA moet een levend document zijn, en moet worden herijkt bij veranderingen.

D. Beheersmaatregelen

Om de risico's van telemetrie voor de werknemers te verlagen, doen wij aan overheidsinstanties en aan DI&I de onderstaande aanbevelingen. Naar ons oordeel is er *op dit moment* sprake van aanvaardbare restrisico's als in ieder geval de dik gedrukte beheersmaatregelen zijn genomen.

Overheidsinstantie

- **Kies voor telemetrieniveau Security.**
- **Voer als daar aanleiding voor is een aanvullende privacyrisicoanalyse uit.**
- Laat medewerkers zoveel mogelijk van Windows gebruik maken met een lokaal account.

SLM Microsoft Rijk (DI&I)

- **Laat Microsoft een verduidelijkend document tekenen waarin in ieder geval de in paragraaf 17.2 benoemde essentiële zaken in klare taal staan beschreven.**
- **Sluit namens de individuele overheidorganisaties een art. 26-overeenkomst met Microsoft.**
- Maak, als je bepaalde risico's als te hoog inschat, aanvullende afspraken met Microsoft.
- Monitor welke gegevensoverdracht er in het kader van telemetrie feitelijk plaatsvindt.

Inleiding

Binnen de Directie Informatievoorziening en Inkoop (DI&I) van het Ministerie van Justitie en Veiligheid (JenV) coördineert het Strategisch Leveranciersmanagement (SLM) Microsoft het afsluiten en onderhouden van het Rijksbrede contractenkader met Microsoft. Dit kader omvat geen afname-afspraken; het is een raamwerk op het niveau van een raamwerkovereenkomst (Microsoft Business and Services Agreement, MBSA) en amendementen (Enterprise Agreements, EA's).

De Microsoftproducten Windows 10 en Office zijn veelgebruikte software binnen de Rijksoverheid. Beide producten maken gebruik van "telemetrie" om diagnostische gegevens over het gebruik van de software met Microsoft te delen. Deze DPIA behandelt Windows 10 Enterprise (versie 1709, en wijzigingen hierop in versie 1803). Technisch gesproken verstuurt een device waar een product op geïnstalleerd is gegevens naar de leverancier, formeel leest de leverancier de gegevens op afstand uit.

SLM Rijk heeft Privacy Management Partners gevraagd om de privacy- en compliance-aspecten van het gebruik van telemetrie binnen Windows 10 Enterprise in kaart te brengen met het oog op het maken van de benodigde afspraken met Microsoft en het kunnen nemen van de vereiste maatregelen door overheidsinstanties die deze software gebruiken.

Deze DPIA is primair een beoordeling van de (privacy)risico's die verbonden zijn aan het verwerken van telemetriegegevens, voor de rijksambtenaren en andere medewerkers van de Rijksoverheid (vrijwel iedereen) die in hun werk gebruik maken van Windows 10. Bijzondere aandacht gaat daarbij uit naar een – weliswaar marginale – beoordeling van de compliance met de Algemene Verordening Gegevensbescherming (AVG) van de verwerking van telemetriegegevens door Microsoft. Aanleiding daarvoor zijn de uitkomsten van een recent onderzoek door de Autoriteit Persoonsgegevens (AP) naar de verwerking van telemetriegegevens in twee andere versies van Windows 10, namelijk Windows 10 Home en Pro. Uit dat onderzoek bleek namelijk dat er vraagtekens kunnen worden gezet bij de bewering van Microsoft dat zij handelt in overeenstemming met de Europese gegevensbeschermingswetgeving. Overigens heeft de AP vorige maand bekend gemaakt dat een herstelplan van Microsoft ertoe heeft geleid dat de geconstateerde overtredingen zijn beëindigd.

In paragraaf 11.2 adviseren wij overheidsinstanties om te kiezen voor telemetrieniveau Security.[1] Er zijn goede redenen om niet voor een hoger niveau van telemetrie te gaan. Aangezien dit al in een vroeg stadium bij het uitvoeren van deze DPIA duidelijk werd, is ervoor gekozen om niet in detail in te gaan op de gegevensverwerking op hogere niveaus en de risico's die daaraan (kunnen) zijn verbonden. Voor de goede orde vermelden wij hier ook dat we in diezelfde paragraaf eveneens uitleggen waarom een keuze voor helemaal geen telemetrie, wellicht enigszins verrassend, leidt tot hogere privacyrisico's dan een keuze voor niveau Security.

Reikwijdte

Deze DPIA had als beoogde reikwijdte de verwerking van telemetriegegevens bij het gebruik van Windows 10 Enterprise, Office en Office 365. Het bleek echter niet mogelijk om voldoende

[1] Zie paragraaf 2.2.1 voor een beschrijving van dit niveau van telemetrie.

betrouwbare informatie over telemetrie bij Office en Office 365 boven water te krijgen.[2] De DPIA beperkt zich daarom noodgedwongen tot Windows 10 Enterprise (versie 1709, en wijzigingen hierop in versie 1803).

Voor dit voorjaar heeft Microsoft een aantal verbeteringen aangekondigd op het gebied van gegevensbescherming bij telemetrie in Windows 10 Enterprise. Die wijzigingen zijn verwerkt in dit rapport.[3] Overigens betreft het hier uitsluitend zaken aan de gebruikerskant, en geen verandering in de verwerking van de gegevens als ze eenmaal bij Microsoft zijn.

Gelet op de moeite die het blijkt te kosten om eenduidige informatie te achterhalen, dient dit DPIA-rapport nadrukkelijk gezien te worden als een 'levend document'. Het is gebaseerd op openbaar beschikbare informatie, aangevuld met door Microsoft tot en met 26 april aangeleverde informatie. Het rapport zal geregeld geactualiseerd dienen te worden, in het bijzonder als Microsoft essentiële wijzigingen doorvoert, zaken anders blijken te liggen dan hier beschreven, of inzichten wijzigen op basis van verkregen nadere informatie.

In een DPIA ligt de focus op de impact van gegevensverwerking op de rechten en vrijheden van betrokkenen. Dat zijn degenen over wie persoonsgegevens worden verwerkt, in dit geval de werknemers die gebruik maken van Microsoft-software. Voor een afgewogen besluit over of, en zo ja hoe, gebruik te maken van Windows, Office en Office 365, zal ook moeten worden gekeken naar de veiligheidsrisico's en de functionaliteitsconsequenties van de verschillende opties. Bij deze nadere beoordeling zouden ook risico's die voortkomen uit het type dienstverlening zoals 'vendor lock in', blokkeren van toegang door de leverancier (lock out) en dienstonderbrekingen moeten worden meegenomen. Dergelijke zaken spelen soms zijdelings een rol in de beoordelingen in deze DPIA, maar zullen zeker ook los daarvan moeten worden beoordeeld. Net zoals voor deze DPIA geldt daarbij dat dit in eerste instantie centraal kan gebeuren door DI&I, maar dat vervolgens iedere individuele overheidsinstantie aanvullend haar eigen afwegingen zal moeten maken.

Deze DPIA is atypisch in die zin dat die niet wordt uitgevoerd door de verwerkingsverantwoordelijke, maar door DI&I als categorieverantwoordelijke voor inkoop van software voor de Rijksoverheid. Om die reden is in deze fase ook de CIO van JenV niet om een reactie gevraagd. De FG van JenV heeft wel meegelezen, en kan zich vinden in de beschrijving en conclusies in dit rapport.

Microsoft zal als belangrijkste verwerkingsverantwoordelijke voor telemetrie zelf ook een DPIA moeten uitvoeren. Daarover zegt het het volgende:

> Microsoft is preparing all of the Impact Assessments for its products and services required by the GDPR. Material information required by our commercial customers in order to prepare their own DPIAs will be shared through the Service Trust Portal prior to the enforcement of the GDPR.

Een overheidsinstantie die, als gebruiker van de software, samen met Microsoft verwerkingsverantwoordelijke is, zal aanvullend daarop een eigen risicobeoordeling moeten uitvoeren. Bij bepaalde geledingen binnen de overheid, denk bijvoorbeeld aan ambassades en consulaten of de inlichtingen- en veiligheidsdiensten, kan er sprake zijn van aanvullende risico's.

De volgende zaken vallen nadrukkelijk buiten de reikwijdte van deze DPIA:
- andere versies van Windows dan Windows 10 Enterprise edition, version 1709/1803;

---

[2] Onder meer doordat het onderzoek van de AP, een belangrijke bron van informatie, uitsluitende gericht was op Windows 10.
[3] Zie in het bijzonder paragraaf 8.5.

  - de aanvullende waarborgen rondom telemetrie waarvan Microsoft heeft aangekondigd dat ze dit voorjaar zullen worden toegevoegd, vallen wel binnen de reikwijdte van de DPIA.
- het eventuele gebruik van telemetriegegevens voor eigen doeleinden door de werkgever;
- het verwerken van functionele gegevens (inhoud van gebruikersbestanden) door Microsoft;[4]
- het feitelijke gebruik van Windows 10 en Office 365, mogelijk ook buiten de werkplek of voor privédoeleinden, door (medewerkers van) een overheidsinstantie;
- het vaststellen of de feitelijke gegevensverwerking door Microsoft overeenkomt met wat Microsoft heeft aangegeven.

Verantwoording

De beoordeling die ten grondslag ligt aan dit rapport is uitgevoerd in de periode maart t/m mei 2018.

De informatie in het rapport is allereerst gebaseerd op openbare informatie, in het bijzonder documentatie van Microsoft op haar website en het onderzoeksrapport van de Autoriteit Persoonsgegevens over telemetrie in Windows 10 Home en Pro. In aanvulling hierop is ook gekeken naar de overeenkomsten die het Rijk met Microsoft heeft. De feiten en beoordelingen zijn in twee workshops met de opdrachtgever besproken. Er is zowel door SSC-ICT als door ministerie van JenV commentaar geleverd. Dit is verwerkt in deze versie.

Vaststellen feiten

Een niet gering probleem bij het uitvoeren van de DPIA bleek te zijn om de feiten duidelijk te krijgen. Er is veel informatie en documentatie beschikbaar vanuit Microsoft, maar deze is verspreid en niet altijd even goed geordend. Problematischer is dat veel van deze teksten onduidelijk of ambigu zijn, en soms zelfs inconsistent lijken.

Al voor aanvang van de DPIA heeft de opdrachtgever een aantal vragen over telemetrie voorgelegd aan Microsoft. De daarop ontvangen antwoorden zijn opgenomen in bijlage 5. Microsoft is ook in de gelegenheid gesteld om schriftelijk te reageren op een tussentijds rapport. Van deze gelegenheid heeft het geen gebruik gemaakt.

Er is nadrukkelijk geen toets gedaan of de feitelijke gegevensverwerking door Microsoft overeenkomt met wat Microsoft zegt te doen. Het blijkt lastig om dat te verifiëren.[5]

Om te voorkomen dat het rapport voortdurend bijgesteld zou moeten worden, is ervoor gekozen om een duidelijk punt in de tijd te markeren voor het vaststellen van het feitencomplex waarop de DPIA gebaseerd is. Dit is de eerder genoemde datum van 26 april van dit jaar.

[4] Er is mede om die reden ook niet gekeken naar het risico van het door Microsoft koppelen van telemetriegegevens aan functionele gegevens (bijv. LinkedIn-profielen). De belangrijkste reden om daar niet op in te gaan is echter dat een dergelijke koppeling in beginsel onrechtmatig is, aangezien er gegevens waarover Microsoft als verwerker resp. verwerkingsverantwoordelijke beschikt gekoppeld zouden worden.

[5] Om dit te kunnen vaststellen heeft de opdrachtgever een testlab ingericht. Daarvan waren bij het sluiten van dit rapport slechts beperkt resultaten beschikbaar.

Terminologie

In dit document spreken we vaak over de overheidsinstantie die zich in haar rol van werkgever een beeld dient te vormen van de privacyaspecten van telemetrie. Afhankelijk van de context duiden we deze eindafnemer aan als “de werkgever”, “de overheidsinstantie” dan wel “de overheidsinstantie (werkgever)”. Zie bijlage 7 voor een overzicht van gebruikte begrippen en bijlage 8 voor een overzicht van de gebruikte afkortingen.

A. Beschrijving kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

Onder A wordt de eerste stap beschreven van de PIA: een overzicht van de relevante feiten van de voorgenomen gegevensverwerkingen. Als de feiten onduidelijk zijn, werkt dit door in de beoordeling.

1. Voorstel

Microsoft verzamelt voortdurend technische prestatie- en gebruiksgegevens over elk apparaat waarop Windows 10 Enterprise is geïnstalleerd.[6] Deze gegevens worden telemetriegegevens genoemd.[7] Microsoft verzamelt via telemetrie bijvoorbeeld allerlei unieke identifiers, in combinatie met gegevens over hard- en software op het apparaat en daarmee verbonden apparaten (zoals routers en printers). Microsoft onderscheidt verschillende niveaus van telemetrie. Het is mogelijk om telemetrie volledig uit te schakelen, maar dat gaat wel ten koste van bepaalde standaard in Windows opgenomen functionaliteit. Dit wordt in paragraaf 2.2 verder uitgewerkt.

Vrijwel alle Nederlandse overheidsinstanties maken gebruik van de genoemde software. Dat stelt ze voor de keuze om ofwel te accepteren dat telemetriegegevens over hun werknemers in zekere mate worden verzameld door Microsoft, ofwel te accepteren dat bepaalde standaard in Windows opgenomen beveiligingsfunctionaliteit niet beschikbaar is.[8]

Deze gegevensbeschermingseffectbeoordeling heeft als doel de verwerking van telemetriegegevens te beschrijven, de rechtmatigheid van de verwerking ervan marginaal te toetsten, en een beeld te vormen van de mogelijke risico's van telemetrie voor de betreffende werknemers, met daaraan gekoppeld de mogelijke beheersmaatregelen die de overheid als inkoper en specifieke overheidsinstanties kunnen nemen om die risico's te verkleinen.

2. Persoonsgegevens

De AVG is slechts van toepassing op de verwerking van 'persoonsgegevens'. Persoonsgegevens zijn gedefinieerd als "alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon".[9]

In haar onderzoek komt de AP tot de conclusie dat alle telemetriegegevens in Window 10 persoonsgegevens zijn:

> Omdat Microsoft meerdere unieke identifiers verbindt aan de telemetriegegevens die zij verzamelt en vastlegt, dienen alle gegevens die Microsoft van en over gebruikers van Windows 10 verzamelt, verkrijgt, genereert en/of in verband met elkaar brengt, te worden aangemerkt als

---

[6] Deze beschrijving is deels ontleend aan die in het onderzoek van de Autoriteit Persoonsgegevens naar telemetrie in Windows 10 Home en Pro.
[7] In een overleg van 1 juni heeft Microsoft aangegeven zelf de term "telemetrie" inmiddels zoveel mogelijk te vermijden, omdat die verwarrend kan werken. Microsoft spreekt als het gaat over de gegevens die het onderwerp van deze DPIA vormen liever over "diagnostische gegevens".
[8] Die beveiligingsfunctionaliteit kan elders ingekocht worden. Dat zal doorgaans een vergelijkbare gegevensstroom met zich meebrengen.
[9] Art. 4(1) AVG.

> persoonsgegevens als bedoeld in artikel 1, onder a, van de Wbp, ongeacht of het gebruikers betreft met een lokaal account, of gebruikers met een Microsoft account.

Deze conclusie geldt evenzeer voor de telemetriegegevens die binnen Window 10 Enterprise worden verwerkt. De conclusie is, hoewel gemaakt vanuit de WBP, onverkort ook relevant onder de AVG.

Hieronder beschrijven we op hoofdlijnen welke persoonsgegevens er worden verwerkt bij telemetrie. Zie bijlage 2 voor details. Alvorens dat te doen, staan we echter eerst stil bij de verschillende typen gegevens zoals Microsoft die definieert.

2.1 Definities

Microsoft verwerkt verschillende typen gegevens over en van gebruikers. Om de contracten, voorwaarden en documentatie van Microsoft goed te kunnen begrijpen, is het essentieel om te weten welke soorten gegevens Microsoft bedoelt als het bepaalde termen gebruikt.

Microsoft geeft aan[10] twee verschillende soorten gegevens te verwerken vanuit apparatuur die is voorzien van een Windows besturingssysteem:
- functionele gegevens
- operationele gegevens

Gelet op hetgeen hierboven is opgemerkt, gaat het in alle gevallen om persoonsgegevens.

De *functionele gegevens* komen voort uit het gebruik van specifieke onderdelen van het Windows platform, zoals Bing (zoekmachine) en Cortona (spraakgestuurde assistent). Daartoe rekent Microsoft ook de gegevens die het verwerkt met het oog op *rights management* (controle of de software onder een geldige licentie gebruikt wordt). Functionele data kan ook voortkomen uit andere programmatuur die door (of voor) de gebruiker wordt geïnstalleerd.

De *operationele gegevens* zijn telemetriegegevens die een diagnostisch doel hebben.

Van sommige gegevens is niet altijd duidelijk in welke categorie ze vallen. Neem als voorbeeld gegevens over de locatie van het apparaat. Microsoft geeft aan dat het hier om functionele data kan gaan, aangezien Windows-gebruikers een gelokaliseerde weersverwachting kunnen krijgen. Niet duidelijk is of locatiegegevens daarmee in de ogen van Microsoft ook altijd als functionele gegevens te beschouwen zijn; en zo nee, hoe Microsoft dan het onderscheid maakt tussen functionele locatiegegevens en operationele locatiegegevens. Evenmin is duidelijk of het bestempelen van gegevens tot "functioneel" betekent dat gebruik ervan voor niet-functionele doeleinden (denk aan combinatie met andere inhoudelijke gebruikersgegevens) is uitgesloten.

Naast 'operationele gegevens' spreekt Microsoft veelal ook van 'diagnostische gegevens'. Niet duidelijk is of die laatste een onderdeel zijn van de operationele gegevens, of dat beide begrippen samenvallen. Het lijkt erop dat "telemetrie" door Microsoft gedefinieerd wordt als de verwerking van diagnostische data. In het vervolg zullen we de termen "diagnostische gegevens" en "telemetriegegevens" door elkaar heen gebruiken.

2.2 Niveaus van telemetrie

Microsoft binnen windows 10 (versie 1709/1803) onderscheidt vijf niveaus van telemetrie:
- Security
- Basic
- Enhanced
- Limited Enhanced
- Full

[10] https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization

Deze niveaus zijn cumulatief, in de zin dat de set van gegevens die op elk niveau worden verwerkt een uitbreiding is van de set van gegevens op het niveau daaronder.

In Windows 10 Enterprise kunnen al deze niveaus worden ingesteld. Alleen de niveaus Basic en Full kunnen door de eindgebruiker als instelling worden gekozen.[11] De andere niveaus kunnen beheerders met behulp van managmenttooling instellen.

De beschreven niveaus worden alleen gebruikt binnen Windows, Windows Server en System Center. En daarnaast in programmatuur die gebruik maakt van de *connected user experiences en telemetry component*. Programmatuur van andere leveranciers, maar ook Microsoft Office, kan ook op een andere wijze communiceren, maar dat valt buiten de scope van dit onderzoek.

2.2.1 Niveau Security[12]

Op het niveau Security worden de volgende gegevens verwerkt vanuit het device die kunnen worden gezien als persoonsgegeven:
- device id
- IP-adres

Deze beide gegevens kunnen door Microsoft worden gecombineerd met direct identificeerbare gegevens, mogelijk ook uit andere verwerkingen dan telemetrie. Beide gegevens zijn daarmee zelfstandig als persoonsgegeven te beschouwen.

Er wordt geen gebruikersdata zoals gemaakte content verzameld. Binnen het niveau Security worden (naar opgave van Microsoft) standaard geen direct identificeerbare gegevens verzameld. Het is echter mogelijk dat in de verzamelde informatie die verstuurd wordt ten bate van de tooling Malicious Software Removal Tool (MSRT) direct herleidbare gegevens zoals een gebruikersnaam of andere gegevens voorkomen indien de gedetecteerde malware deze gegevens bevat. Windows update informatie wordt op dit niveau niet uitgewisseld met Microsoft. De standaard Windows update voorziening zal hierdoor niet functioneren. Bij dit niveau zal binnen de eigen omgeving een Windows Server Update Services (WSUS) moeten worden ingericht om de devices te voorzien van updates. De diensten Windows Server Update Services (WSUS) en System Center Configuration Manager worden niet beïnvloed door keuze voor dit niveau

2.2.2 Niveau Basic

Op het niveau Basic worden de gegevens van niveau Security verzameld, aangevuld met:
- IMEI nummer
- gebruik van programma's (compatability data)

Het niveau Basic bevat hiernaast ook uitgebreide gegevens over de hardware- en softwareconfiguratie van de apparaten, gegevens over het functioneren van Windows op het apparaat (hoe vaak Windows is vast gelopen, hoe vaak Windows een zogenaamde "hang-up" heeft gehad). Het is mogelijk dat op basis van de combinatie van deze gegevens een uniek profiel ('device fingerprint') van een systeem gemaakt kan worden, waardoor een systeem identificeerbaar is of kan zijn.

Indien de Microsoft store wordt gebruikt binnen het platform zullen hier tevens gegevens voor worden verzameld die nodig zijn voor het leveren van licenties uit deze omgeving, en het daadwerkelijke gebruik van de store zoals openen van de applicatie, gebruik statistieken etc.

---

[11] In de praktijk zal deze mogelijkheid echter door de werkgever uitgeschakeld worden. Zie paragraaf 3.
[12] https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization#diagnostic-data-levels

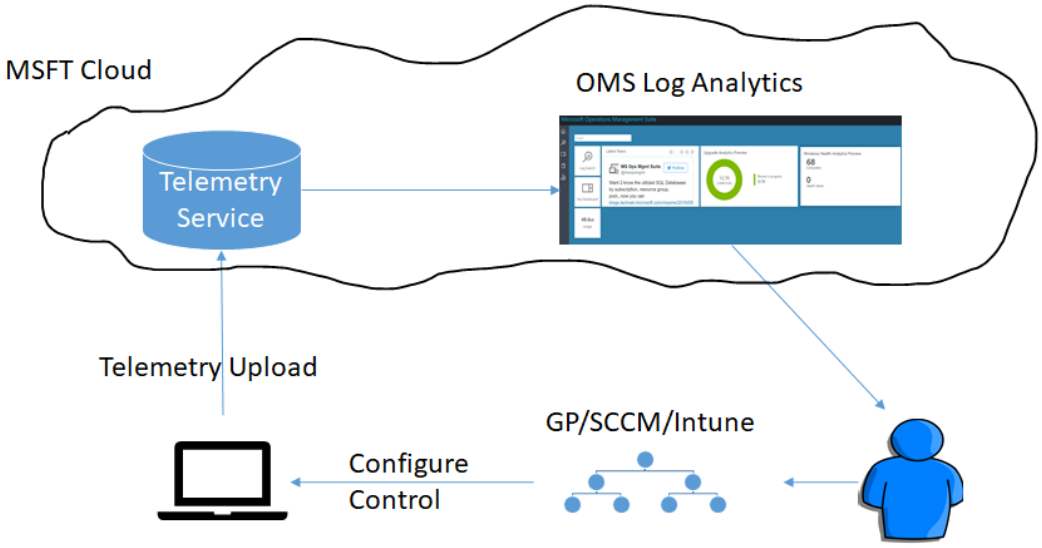
Deze niveaus geven geen veranderingen aan de functionele data die verstuurd wordt naar Microsoft. Echter, ook hierin kunnen indirecte identificeerbare gegevens worden verstuurd. Als voorbeeld geeft Microsoft aan dat Windows ten behoeve van het laten zien van het huidige weerbeeld de locaties van het apparaat als functionele data ziet. Deze gegevens zouden kunnen worden gecombineerd met andere gegevens, en hierdoor wel een persoonsgegevens zijn. Het is dus van belang ook deze gegevens in het kader van deze analyse mee te wegen.

2.2.3 Niveaus Enhanced en Limited Enhanced[13]

Op het niveau Enhanced (het standaard ingestelde niveau in Windows 10 Enterprise) worden alle gegevens van beide eerdere niveaus verzameld, aangevuld met;

- Extra diagnostische data zoals systeem-, applicatie- en hardware-log events.
- Chrashdumps
- Windows Analytics Device Health reports

Door het Windows-onderdeel *connected user experience and telementry component* worden zogenaamde *crash dumps* verstuurd (deze bevatten geen volledige kopie van het geheugen in de vorm van *heap/full dumps*). Het is zeker niet uit te sluiten dat crash dumps additionele gegevens bevatten, zoals gebruikersnaam, ingelogde gebruiker, mailadressen, enz. Deze extra gegevens ten opzichte van het niveau Basic worden volgens opgave van Microsoft gebruikt ten behoeve van productverbeteringen. Hiernaast kunnen de verzamelde gegevens door de beheerder van de omgeving worden gebruikt als bron voor "Windows Analytics Device Health reports[14]". Dit is een dienst van Microsoft binnen de op de cloud gebaseerde Operations Management Suite (OMS). Met de gegevens kunnen Windows devices worden geïdentificeerd die problemen hebben, zoals crashes, slechte drivers en onvolkomenheden in de configuratie van Windows Information Protection (WIP).



[13] https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization#diagnostic-data-levels

[14] Zie voorbeeld Bijlage 10

In de hier onderzochte versie van Windows 10 (build 1709) is ten bate van deze functionaliteit een additioneel niveau geïntroduceerd: *Limited Enhanced*. Hierbij wordt in tegenstelling tot het hiervoor beschreven niveau alleen die diagnostische data verzameld die minimaal nodig is voor de beschreven "Windows Analytics Device Health reports" dienst. Dit betekent dat de hoeveelheid datapunten die worden verzameld en verstuurd tussen die van de niveaus Basic en Enhanced in ligt. Er worden minder systeemevents verstuurd, en de verstuurde crash dumps bevatten geen kopieën van het geheugen.

2.2.4 Niveau Full[15]

Het niveau Full is het standaard niveau voor de windows Pro versie. En hiernaast ook relevant bij een device/gebruiker die heeft aangegeven (opt-in) onderdeel te willen zijn van het Windows insider programma. Hierin krijgen gebruikers eerder dan de generieke gebruikers van Windows updates aangeboden. Aansluiten bij het Windows insider programma wordt ten stelligste afgeraden voor andere dan testsystemen. In het kader van dit onderzoek is relevant dat in dit niveau niet alleen data wordt verzameld door van te voren ingestelde Windows-onderdelen (Connected User Experiences and Telemetry component, Windows Error Reporting, Online Crash Analysis en OneDrive app for Windows 10) maar dat Microsoft ook zelfstandig programmatuur op het device kan gebruiken om gegevens te verzamelen. Deze gegevens zijn veelomvattend, en kunnen daarmee ook zeer veel gegevens van de gebruiker bevatten. Een Windows-apparaat onderdeel laten zijn van het Windows Insider programma wordt om deze reden, en vanwege mogelijke verstoringen in of aan productiesystemen, afgeraden voor gebruikers buiten een test-omgeving of andere strikt beheerde omgeving.

2.2.5 Detail-instellingen, Zero Emission script

Naast de hierboven beschreven vijf standaardniveaus biedt Microsoft ook nog een zogenaamd "Zero Emission" script aan. Daarmee kan de beheerder er gradueel voor kiezen om specifieke dataoverdrachten te laten plaatsvinden. Het script maakt het mogelijk om 28 specifieke onderdelen[16] van het Microsoft platform toestemming te geven om gegevens te verzamelen en te versturen. Het is ook mogelijk om met behulp van dit script de overdracht van telemetriegegevens geheel te blokkeren.[17] [18] Het moet worden geïmplementeerd binnen de eigen IT omgeving, en wordt standaard door Microsoft geleverd.

Alle in het kader van telemetrie verwerkte gegevens zijn aan te merken als persoonsgegevens.

2.3 Typen verwerkte gegevens

Hierboven is op hoofdlijnen beschreven welke gegevens er worden verwerkt in het kader van telemetrie. Vervolgens is de vraag hoe deze gegevens te duiden zijn in termen van de

---

[15] https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization#diagnostic-data-levels

[16] https://docs.microsoft.com/en-us/windows/configuration/manage-connections-from-windows-operating-system-components-to-microsoft-services.

[17] Door het uitschakelen van telemetrie zullen, in meer of minder mate, specifieke diensten niet meer functioneren. Zie paragraaf 6.

[18] In een overleg van 1 juni heeft Microsoft aangegeven dat het ook met het Zero Emissions script niet mogelijk is om als werkgever alle overdracht van telemetriegegevens van je werknemers helemaal te stoppen. Wel wordt eraan gewerkt om de mogelijkheden voor de werkgever op dat vlak

gegevensbeschermingswetgeving. Zoals in de toelichting bij dit onderdeel is benoemd, gaat het dan om de vraag of er bij telemetrie bijzondere of strafrechtelijke gegevens worden verwerkt, of wettelijk voorgeschreven identificatienummers.

In de context van telemetrie is het echter zeker zo relevant dat telemetriegegevens vallen onder de definitie van "informatie in de randapparatuur van een gebruiker" uit de Telecommunicatiewet (Tw).

2.3.1 Bijzondere en strafrechtelijke gegevens

In het kader van telemetrie verzamelt Microsoft niet gericht bijzondere of strafrechtelijke persoonsgegevens. Niettemin zijn er twee oorzaken waardoor dit soort gegevens bij telemetrie toch verwerkt kunnen worden:

- Het kan voorkomen dat er bij telemetrie als "bijvangst" functionele gegevens verwerkt worden, bijvoorbeeld als er volledige crash (en heap) dumps worden gemaakt. De mogelijke inhoud van deze gegevens is alleen beperkt door wat de gebruiker wel of niet met de software doet. Er kunnen dus ook bijzondere of strafrechtelijke gegevens tussen zitten, over de gebruiker zelf of over burgers waarover hij met de software gegevens verwerkt.
- Sommige systeemkenmerken worden weliswaar verzameld ten behoeve van de algemene telemetriedoeleinden, maar kunnen naar hun aard niettemin bijzonder zijn. Wij denken hier met name aan gegevens over toegankelijkheidsinstellingen, die gezondheidsinformatie over de gebruiker kunnen prijsgeven. Op niveau Security worden dergelijke gegevens niet verwerkt.

2.3.2 Gegevens van gevoelige aard

Naast bijzondere gegevens kan er ook sprake zijn van de verwerking van "gegevens van gevoelige aard". De AP geeft in haar onderzoeksrapport aan dat deze informele kwalificatie iets zegt over de impact die het gegeven kan hebben, en daarmee over de verenigbaarheid van verdere verwerking van deze gegevens, en van de omvang van de verplichting om betrokkenen te informeren. Volgens de AP zijn onder meer gegevens over appgebruik en surfgedrag te beschouwen als gegevens van gevoelige aard. Deze specifieke gegevens van gevoelige aard worden overigens niet verwerkt op de niveaus Security en Basic, wel op de meeromvattende niveaus. Uiteraard is ook voor deze gegevens niet uit te sluiten dat ze als bijvangst worden verwerkt.

2.3.3 Wettelijk voorgeschreven identificatienummers

In de huidige Europese privacyrichtlijn krijgen wettelijk voorgeschreven nummers ter identificatie van personen extra bescherming. Deze extra bescherming vervalt als verplichting met de komst van de AVG, maar blijft in Nederland niettemin bestaan omdat zij is opgenomen in de Uitvoeringswet AVG.

Wettelijk voorgeschreven identificatienummers worden in het kader van telemetrie niet gericht verzameld door Microsoft. Ook van deze gegevens is echter niet uit te sluiten dat deze in een volledige crash (en heap) dump aanwezig zou kunnen zijn.

---

te vergroten.

Telemetriegegevens kunnen bijzondere gegevens, strafrechtelijke gegevens, gegevens van gevoelige aard en wettelijk voorgeschreven identificatienummers omvatten. Zulke gegevens worden op niveau Security echter niet gericht verzameld.

2.3.4 Informatie in de randapparatuur van een gebruiker

Zoals is uitgewerkt in paragraaf 9 is de Telecommunicatiewet (Tw) beperkt van toepassing op de verwerking van telemetriegegevens:

- de regels voor verkeersgegevens, locatiegegevens en diensten met toegevoegde waarde zijn niet van toepassing, aangezien Microsoft de telemetriegegevens niet verwerkt in de hoedanigheid van telecomprovider[19];
- de regels voor het opslaan van en toegang krijgen tot informatie in de randapparatuur van een gebruiker zijn wel van toepassing, aangezien het voor deze regels niet van belang is of de verwerking al dan niet geschiedt door een telecomprovider.

Het is hier dus niet nodig om nader in te gaan op de verwerking van verkeersgegevens en locatiegegevens als onderdeel van telemetrie.

Op het opslaan van of toegang verkrijgen tot informatie in de randapparatuur van een gebruiker is artikel 11.7a Tw van toepassing. [20] Of de verwerking van telemetriegegevens door Microsoft daaraan voldoet, bespreken we in paragraaf 11.

Telemetrie valt onder de reikwijdte van bepalingen in de Telecommunicatiewet en in de toekomstige e-Privacyverordening over het verkrijgen van toegang tot informatie in de randapparatuur van een gebruiker.

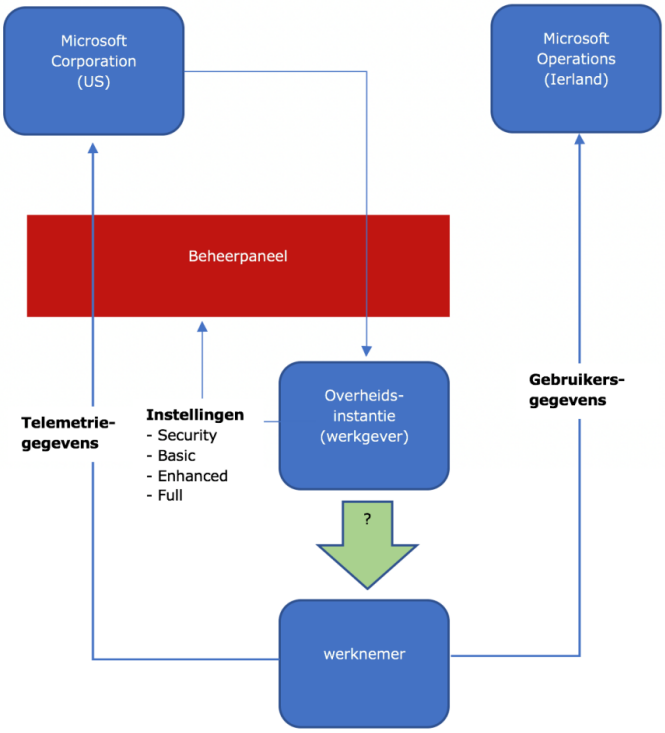
3. Gegevensverwerkingen

Bij de verwerking van telemetriegegevens in Windows 10 Enterprise zijn de volgende actoren betrokken:
- Microsoft
- Het ministerie van JenV (SLM Rijk)
- de overheidsinstantie

Dit wordt verder uitgewerkt in paragraaf 5.

Schematisch zien de gegevensstromen eruit als weergegeven in onderstaand diagram. Voor de volledigheid is daarin ook de stroom van gebruikersgegevens weergegeven, die buiten de reikwijdte van deze DPIA valt. Deze DPIA richt zich zoals benoemt in de inleiding alleen op de telemetrie verkeersstroom.

.



- Het apparaat van de werknemer stuurt de gebruikersgegevens naar het datacentrum van Microsoft Operations in Ierland.
- Microsoft Corp. in de VS leest telemetriegegevens van het apparaat van de werknemer uit en slaat deze lokaal (dus in de VS) op. De werkgever beslist via het beheerpaneel[21] welke typen telemetriegegevens Microsoft Corp. kan uitlezen. Er zijn vijf niveaus: Security, Basic, Limited Enhanced, Enhanced en Full. Hoe hoger het niveau, hoe meer gegevens Microsoft Corp krijgt.
    - Technisch gezien is er alleen op niveau Full sprake van een actieve handeling van Microsoft op het apparaat. Op de andere niveaus loopt de gegevensstroom alleen van het apparaat naar Microsoft Corp. Doordat Microsoft de configuratie van de op het apparaat aanwezige software component kan wijzigen, is er ondanks dat het technisch om een upload van het apparaat naar Microsoft gaat, wel sprake van een vorm van uitlezen.
- Microsoft stelt een deel van de telemetriegegevens beschikbaar aan de werkgever via het beheerpaneel.[22] [23]
- De werkgever kan de telemetriegegevens voor eigen doeleinden gebruiken, bijvoorbeeld voor het evalueren van prestaties, aanwezigheid of gedrag van de werknemer.

Toelichting verdient hier met name de pijl van de werkgever naar het beheerpaneel. Windows 10 zit zo in elkaar dat de eindgebruiker (werknemer) in principe zelf het telemetrieniveau kan instellen. In Windows 10 Enterprise versie 1803 wordt een gebruiker standaard de keuze geboden te kiezen

[21] In een overleg van 1 juni heeft Microsoft aangegeven dat dit niet via een 'beheerpaneel' gebeurt, maar via verschillende mogelijkheden voor beheerders, zoals 'group policies'. Vgl. de betreffende antwoorden in bijlage 5.
[22] https://docs.microsoft.com/en-us/windows/deployment/update/windows-analytics-overview.
[23] In een overleg van 1 juni heeft Microsoft aangegeven dat alleen het programma Windows Analytics toegang geeft tot "client data", en dat deze geen rechtstreekse toegang biedt tot de telemetriedatabase.

tussen niveau Enhanced en niveau Basic. De werkgever kan dit echter beperken of zelfs onmogelijk maken door op beheerniveau deze keuze aan de werknemer op te leggen. De opdrachtgever heeft aangegeven dat overheidsinstanties er om redenen van informatie- en staatsveiligheid altijd voor zullen kiezen om telemetrie-instellingen inderdaad geheel op organisatieniveau te beheren. De individuele werknemer heeft dus in de praktijk geen enkele keus.

In het schema staat niet expliciet benoemt dat er een mogelijke stroom is vanuit Microsoft Corp naar derden, echter Microsoft geeft zelf aan dat[24]:

> *Microsoft does not share personal data of our customers with third parties, except at the customer's discretion or for the limited purposes described in the Privacy Statement[25]. Microsoft may share business reports with OEMs and third-party partners that include aggregated and anonymized diagnostic data information. Data-sharing decisions are made by an internal team including privacy, legal, and data management.*

Het is dus wel mogelijk dat een beperkte gegevensstroom bestaat. Er is geen reden om aan te nemen dat deze gegevensstroom voor andere doelen dan de benoemde gebruikt wordt.

Niet duidelijk is in hoeverre telemetriegegevens door Microsoft Corp. gedeeld worden met andere bedrijfsonderdelen.

3.1 Endpoints

Telemetriegegevens (en andere gegevens) die door Microsoft verzameld worden, kunnen op verschillende plekken bij Microsoft terecht komen, de zogeheten "endpoints".

Microsoft zegt hierover het volgende:[26]

> *Some Windows components, apps, and related services transfer data to Microsoft network endpoints. Details about the different ways to control traffic to these endpoints are described in* Manage connections from Windows operating system components to Microsoft services*. You can evaluate which other connections Windows makes to Microsoft services and determine whether or not to turn them off in your environment.*

Dit is verder uitgewerkt in paragraaf 8.

[24] https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization

[25] https://privacy.microsoft.com/nl-NL/privacystatement

[26] Annex 1.

4. Verwerkingsdoeleinden

Over de doeleinden van telemetrie in Windows 10 Enterprise zegt Microsoft het volgende:[27]

> Windows diagnostic data is vital technical data from Windows devices about the device and how Windows and related software are performing. It's used in the following ways:
> - Keep Windows up to date
> - Keep Windows secure, reliable, and performance
> - Improve Windows – through the aggregate analysis of the use of Windows
> - Personalize Windows engagement surfaces

Het lijkt erop dat in Windows Enterprise telemetrie niet voor direct marketing gebruikt wordt.[28] [29] Het is wel mogelijk dat programmatuur, zoals de internetbrowser Microsoft Edge, op basis van andere middelen dan telemetrie (zoals cookies) gegevens verwerken voor marketingdoeleinden.

De eventuele verwerking van telemetriegegevens door de werkgever valt buiten de reikwijdte van deze DPIA.

Microsoft zegt telemetrie in Windows 10 Enterprise toe te passen voor de volgende doeleinden:

- **Windows actueel houden;**
- **Windows veilig en betrouwbaar houden;**
- **de prestaties van Windows op peil houden;**
- **Windows verbeteren op basis van statistische analyses over het gebruik;**
- **de interacties van gebruikers met het systeem personaliseren.**

5. Betrokken partijen

De AVG kent twee fundamentele rollen bij de verwerking van persoonsgegevens, ieder met zijn eigen verantwoordelijkheden en verplichtingen:

- de verwerkingsverantwoordelijke: de natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;
- de verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

---

[27] https://docs.microsoft.com/nl-nl/windows/configuration/configure-windows-diagnostic-data-in-your-organization.

[28] Mocht deze conclusie in algemene zin onjuist blijken, dan is direct marketing op basis van telemetriegegevens mogelijk niettemin niet toegestaan gelet op de contractuele afspraken tussen Microsoft en de Nederlandse overheid. Dit hangt echter af van de precieze reikwijdte van de term “Gegevens van de klant” in het amendement op het MBSA, en die is niet duidelijk.

[29] In een overleg van 1 juni heeft Microsoft aangegeven dat het Reclame ID wel degelijk verwerkt kan worden (en standaard verwerkt wordt) binnen Windows Enterprise, zowel door eigen programma’s als door apps van derde partijen.

Deze definities zijn door de Artikel 29 Werkgroep verder uitgewerkt in Opinie 1/2010 inzake de begrippen 'verantwoordelijke' en 'verwerker' (Opinie WP169). De Artikel 29 Werkgroep stelt: "The concept of controller is a functional concept, intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis." In de bijlage is een memo opgenomen die nader ingaat op de situatie waarbij er meer dan één verantwoordelijke is voor dezelfde gegevensverwerking. Naast verdere duiding van gehanteerde begrippen (formele, functionele en feitelijke verantwoordelijke) beschrijft de memo tevens de verschillende onderlinge relaties tussen de 'medeverantwoordelijken' en bijbehorende vormen van aansprakelijkheid.

Wij komen voor de verwerking van telemetriegegevens tot de volgende conclusies voor wat betreft de rollen van Microsoft, JenV(SLM Rijk) en de overheidsinstanties (werkgevers):

- *Het apparaat dat ter beschikking is gesteld van de werknemer stuurt de gebruikersgegevens naar het datacentrum van Microsoft Operations in Ierland.*
  De werkgever is de verwerkingsverantwoordelijke voor deze gegevens, en Microsoft Operations Ierland is de verwerker.
- *Microsoft Corp. in de VS leest telemetriegegevens van het apparaat van de werknemer uit en slaat deze lokaal (dus in de VS) op. De werkgever beslist via het beheerpaneel welke typen telemetriegegevens Microsoft Corp. kan uitlezen. Er zijn vijf niveaus: Security, Basic, Limited Enhanced, Enhanced en Full. Hoe hoger het niveau, hoe meer gegevens Microsoft Corp kan uitlezen.*
  Voor deze gegevens is Microsoft Corp. de verwerkingsverantwoordelijke, en de werkgever is de medeverwerkingsverantwoordelijke (feitelijke verantwoordelijke, WP169). In het licht van art. 26 AVG zijn er daarom afspraken nodig tussen Microsoft Corp. en de werkgever waarin wordt uitgewerkt hoe beide verwerkingsverantwoordelijken hun respectievelijke AVG-verplichtingen naleven en de verantwoordelijkheden verdelen.
- *Microsoft stelt een deel van de telemetriegegevens beschikbaar aan de werkgever via het beheerpaneel.*
  Dit komt neer op een derdenverstrekking van Microsoft Corp. aan de werkgever. Microsoft is de verwerkingsverantwoordelijke voor het verstrekken van de gegevens, de werkgever voor het ontvangen (en verder verwerken) ervan.
- *De werkgever kan de telemetriegegevens voor eigen doeleinden gebruiken, bijvoorbeeld voor het evalueren van prestaties, aanwezigheid of gedrag van de werknemer.*
  Voor dit gebruik is de werkgever de enige verwerkingsverantwoordelijke. De specifieke beoordeling van de rechtmatigheid van deze verwerking door de werkgever is geen onderdeel van deze DPIA

Microsoft Corp. is de verwerkingsverantwoordelijke voor telemetrie, en de werkgever is de medeverwerkingsverantwoordelijke. Op grond van art. 26 AVG moeten beide partijen daarom onderlng afspraken maken en die schriftelijk vastleggen.

De betrokkenen bij de verwerking van telemetriegegevens zijn primair de werknemers die gebruik maken van Windows. Wanneer er als bijvangst van telemetrie (gedeeltelijke) inhoud van bestanden wordt verwerkt, kan het gaan om de gegevens van willekeurige individuen die enigerlei vorm van relatie hebben met de betreffende overheidsinstantie.

Microsoft geeft aan dat intern telemetriegegevens alleen toegankelijk zijn voor diegenen voor wie dat functioneel noodzakelijk is. Niet duidelijk is of, en zo ja in hoeverre, Microsoft bij telemetrie gebruik maakt van verwerkers of telemetriegegevens beschikbaar stelt aan andere verwerkingsverantwoordelijken.

6. Belangen bij de gegevensverwerking

6.1 Belangen Microsoft

De belangen van Microsoft bij de verwerking van telemetriegegevens zijn in eerste instantie af te leiden uit de doelstellingen van de verwerking daarvan zoals die zijn weergegeven in paragraaf 4. Essentiëler is echter de strategische transitie die Microsoft aan het doormaken is, waarbij Windows niet langer als een product maar als een dienst wordt gezien. Er is hierdoor ook een mogelijkheid ontstaan dat het stoppen met het leveren van de dienst gevolgen heeft voor haar afnemers.

Microsoft zegt hier zelf het volgende over:

> ***Understanding Windows diagnostic data***
>
> *Windows as a Service is a fundamental change in how Microsoft plans, builds, and delivers the operating system. Historically, we released a major Windows version every few years. The effort required to deploy large and infrequent Windows versions was substantial. That effort included updating the infrastructure to support the upgrade. Windows as a Service accelerates the cadence to provide rich updates more frequently, and these updates require substantially less effort to roll out than earlier versions of Windows. Since it provides more value to organizations in a shorter timeframe, delivering Windows as a Service is a top priority for us.*
>
> *The release cadence of Windows may be fast, so feedback is critical to its success. We rely on diagnostic data at each stage of the process to inform our decisions and prioritize our efforts."*

6.2 Belangen JenV DI&I

DI&I heeft als belang om de overheidsinstanties ten behoeve waarvan zij handelt te ondersteunen bij een goede en efficiënte bedrijfsvoering.

6.3 Belangen overheidsinstantie (werkgever)

De overheidsinstantie die Windows 10 gebruikt, ziet zich geconfronteerd met tegengestelde belangen.

Aan de ene kant dient zij zich te gedragen als goed werkgever.[30] Concreet betekent dat in deze context eerst en vooral dat zij haar werknemers niet moet verplichten tot onnodige verwerking van hun gegevens.

Anderzijds moet zij het haar werknemers echter ook zo gemakkelijk mogelijk maken, onder meer door het beschikbaar stellen van hulpmiddelen, zoals software, om veilig, efficiënt en effectief te werken. Windows 10 is juist daarvoor bedoeld. Door het uitschakelen van telemetrie zullen echter, in meer of minder mate, specifieke diensten niet meer functioneren. Microsoft geeft hierbij als voorbeeld[31] dat voor de werking van Windows Defender minimaal een gegevensoverdracht op niveau Security benodigd is om deze specifieke toepassing te voorzien van zogenaamde "signature"- en detectievernieuwingen.

In aanvulling hierop geeft Microsoft aan[32] dat telemetrie haar klanten (indirect) helpt om zich voor te bereiden op aanvallen die tot datalekken kunnen leiden, en om zulke aanvallen op te sporen en zich ertegen te verdedigen. Ook geeft Microsoft het beoordelen of een klant klaar is voor een

---

[30] Zie paragraaf 9

[31] https://docs.microsoft.com/en-us/windows/configuration/configure-windows-diagnostic-data-in-your-organization#understanding-windows-diagnostic-data

[32] https://docs.microsoft.com/nl-nl/windows/configuration/configure-windows-diagnostic-data-in-your-organization.

upgrade ("upgrade readiness") als een voorbeeld van hoe ook de klant voordeel kan hebben van haar verwerking van telemetriegegevens.

Microsoft stelt de telemetriegegevens via een dashboard en andere tools ook beschikbaar voor de werkgever. Dit brengt twee aanvullende privacyaspecten met zich mee:

- De werkgever kan deze gegevens over zijn werknemers voor eigen doeleinden verwerken, bijv. als personeelsvolgsysteem of om te controleren op niet-toegestane handelingen. Dit eventuele gebruik van telemetriegegevens door de werkgever valt buiten de reikwijdte van deze DPIA. De werkgever zal hierop zelf een privacy risicobeoordeling moeten uitvoeren.
- Zelfs wanneer de werkgever de telemetriegegevens geheel niet voor eigen doeleinden wil verwerken, is het waarschijnlijk onvermijdelijk dat beheerders aan zijn kant in beginsel toegang kunnen krijgen tot de telemetriegegevens. Daardoor ontstaat een informatiebeveiligingsrisico. Indien de klant inderdaad niet de intentie of behoefte heeft om de telemetriegegevens zelf te gaan verwerken, dan ligt dit risico aan de kant van Microsoft.

Microsoft heeft als kernbelang het kunnen leveren van veilige en betrouwbare software, mede in het licht van de transitie van leverancier van producten naar leverancier van diensten.

De overheidswerkgever heeft potentieel conflicterende belangen: enerzijds effectief en veilig werken mogelijk maken, anderzijds bovenmatige verwerking van gegevens van werknemers voorkomen.

7. Verwerkingslocaties

Telemetriegegevens worden doorgegeven naar Microsoft Corp. Niet bekend is waar het deze gegevens verwerkt.

Het is niet duidelijk in welke landen Microsoft telemetriegegevens verwerkt.

8. Techniek en methode van gegevensverwerking

8.1.1 Gegevensverzameling[33]

Windows 10 en Windows Server 2016 zijn uitgerust met het zogenaamde Connected User Experiences en Telemetry component. Deze component gebruikt "Event Tracing for Windows (ETW)" tracelogging om events en diagnostische data te verzamelen en op te slaan. Het is een Windows1 0 specifieke loggingtechnologie die niet exclusief is voor de telemetrie. De Tracelogging component kan ook worden aangeroepen door andere componenten van het besturingssysteem.

Verzamelde gegevens worden, afhankelijk van het ingestelde telemetrieniveau door de Connected User Experiences and Telemetry component verstuurd naar Microsoft. De planning van het uploaden van de gegevens is afhankelijk van een aantal specieke attributen van het gebruik van het apparaat (gebruikt netwerk, proces prioriteit, gebruik batterij). Alleen gegevens van realtime events zoals Windows Defender Advanced Threat Protection gebeurtenissen (virus alerts e.d.) worden direct verstuurd. Als het Windows-apparaat gebruik maakt van een mobiel netwerk (metered netwerk) worden normale events niet verstuurd. Bij gebruik van een reguliere

[33] https://docs.microsoft.com/nl-nl/windows/configuration/configure-windows-diagnostic-data-in-your-organization.

netwerkverbinding wordt elke vier uur (indien op batterij) of elke 15 minuten een bestand verstuurd. Diagnostische gegevens en crash data worden alleen verstuurd als het devivce niet op batterij werkt en gebruik maakt van een regulier netwerk.

Alle verstuurde gegevens worden versleuteld met SSL met certificate pinning[34] gedurende het versturen van het device naar de Microsoft Data Management Service. Door gebruik te maken van certificate pinning is het niet mogelijk om met een zogenaamd Man in the Middle aanval de gegevens te onderscheppen.

8.1.2 Verbindingen

Op een Windows-apparaat maakt de Connected User Experiences en Telemetry component verbinding met de Microsoft Data Management-service op https://v10.vortex-win.data.microsoft.com. De ontvangen gegevens worden vervolgens binnen het Microsoftnetwerk verstuurd naar een eigen cloudomgeving. Toegang tot deze gegevens wordt afgeschermd vanuit een *least privileged* principe. Alleen medewerkers van Microsoft met een geldige noodzaak hebben toegang tot de telemetriegegevens.

De volgende tabel geeft een overzicht van de eindpunten van de verbindingen van de verbindingen die worden gebruikt door het Connected User Experiences and Telemetry component:

Windows release	**Endpoint**
Windows 10, versions 1703 and 1709	Diagnostics data: v10.vortex-win.data.microsoft.com/collect/v1 Functional: v20.vortex-win.data.microsoft.com/collect/v1 Windows Advanced Threat Protection is country specific and the prefix changes by country for example: **de**.vortex-win.data.microsoft.com/collect/v1 settings-win.data.microsoft.com

Hiernaast zijn voor andere diagnostische data (niet vanuit Connected User Experiences and Telemetry component) de volgende eindpunten relevant:

Service	**Endpoint**
Windows Error Reporting	watson.telemetry.microsoft.com
Online Crash Analysis	oca.telemetry.microsoft.com
OneDrive app for Windows 10	vortex.data.microsoft.com/collect/v1

[34] https://tools.ietf.org/html/draft-ietf-websec-key-pinning-21

8.1.3 Gebruik van en toegang tot diagnostische gegevens

Het least privileged toegangsprincipe is de norm voor toegang tot diagnostische data. Microsoft deelt geen persoonlijke gegevens van klanten met derde partijen anders dan wanneer hier zelf voor kiest of voor de gelimiteerde doeleinden die zijn beschreven in het Privacy Statement. [35]Microsoft kan geaggregeerde of geanonimiseerde diagnostische rapporten delen met OEMs en derde partijen

8.2 Bijzondere typen verwerkingen

Wij beschikken niet over specifieke informatie of er sprake is van (semi-)geautomatiseerde besluitvorming, profilering of big data-verwerkingen door Microsoft. Het moge echter duidelijk zijn dat de centrale verwerking van telemetriegegevens van Windows 10-gebruikers onder de noemer 'big data' valt. Verder is de laatste van de in paragraaf 4 beschreven doeleinden van Microsoft gericht op individuele gebruikers. Gelet op de vele data die er worden verzameld, is het dan onwaarschijnlijk dat voor het verwezenlijken van die doelstellingen geen gebruik wordt gemaakt van geautomatiseerde besluitvorming of profilering.

Telemetrie is een vorm van 'big data'. Verder mag worden aangenomen dat Microsoft bij telemetrie gebruik maakt van geautomatiseerde besluitvorming, waaronder profilering

8.3 Informatiebeveiliging

In het kader van deze DPIA is door Privacy Management Partners geen onderzoek gedaan naar het bestaan en de werking van de beveiligingsmaatregelen bij het verwerken van telemetriegegevens door Microsoft. Wel zijn in het algemeen de beveiligingsmaatregelen bekeken die Microsoft heeft getroffen. Daarbij is door Microsoft de onderstaande informatie verstrekt.

- Het versturen van de gegevens gebeurt middels een versleutelde verbinding (SSL) Deze verbinding gebruikt certificate pinning als waarborg.
- De gegevens worden bewaard in de microsoft cloud omgeving, toegang tot de gegevens is gebaseerd op het principe van "least privileged" en alleen medewerkers voor wie toegang valide is vanuit hun business rol hebben toegang tot gegevens.
- Persoonsgegevens worden alleen gedeeld met een derde als er toestemming is gegeven door de klant. Microsoft deelt verder alleen geaggregeerde en geanonimiseerde gegevens met derden.
- De bewaartermijn van de diagnostische gegevens is 30 dagen. Specifieke gegevens (error reporting, en aankoophistorie) worden langer bewaard.

De Microsoft cloud omgeving voldoet aan reguliere normenkaders op het gebied van informatiebeveiliging en gegevensbescherming zoals ISO 27001 en ISO 27018. De producten Microsoft Azure (cloud) en Office 365 zijn gecertificeerd op basis van ISO 27001. Voor beide producten zijn SOC type 1, 2 en 3 assurance rapporten[36] beschikbaar.

---

[35] https://privacy.microsoft.com/nl-nl/privacystatement

[36] SOC 1 – assurancerapport over interne beheersing bij IT-serviceorganisaties in relatie tot de financiële verslaggeving, bedoeld voor de klanten van de serviceorganisatie en hun toezichthouders;
SOC 2 – assurancerapport over interne beheersing bij IT-serviceorganisaties, bedoeld voor de klanten van de serviceorganisatie en hun toezichthouders;
SOC 3 – verkort assurancerapport over interne beheersing bij IT-serviceorganisaties bedoeld voor het algemeen verkeer.

Naar aanleiding van het bovenstaande, de certificeringen en de afgegeven assurance hebben wij geen reden om aan te nemen dat de beveiligingsmaatregelen aan de zijde van Microsoft niet passend zouden zijn.

8.4 Hulpmiddelen voor de klant en eindgebruiker

Microsoft heeft aangekondigd in de "Spring 2018 release" een drietal nieuwe features te implementeren die beide moeten zorgen voor meer transparantie met betrekking tot het gebruik van telemetrie gegevens door Microsoft:

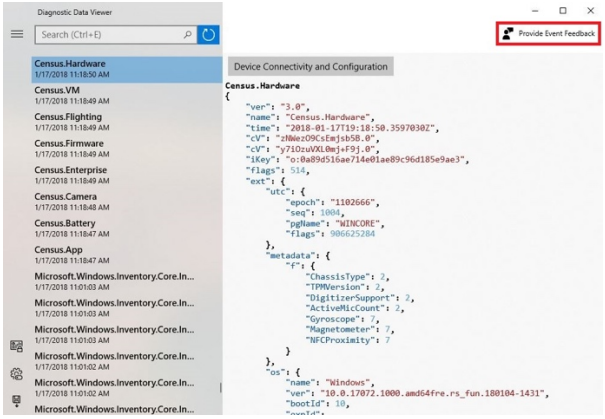
- Delete by device ID
- Diagnostic Data Viewer
- Configuratie-instellingen

De eerste twee features zijn gericht op de eindgebruiker van het Windows operating systeem. Daarmee is de toegevoegde waarde ervan in een Enterprise omgeving mogelijk beperkt. Verder zijn deze features gericht op het vergroten van de transparantie en controle voor de gebruiker. Ze hebben geen invloed op de verwerking van telemetriegegevens als die eenmaal zijn verzameld.

8.4.1 Diagnostic data viewer

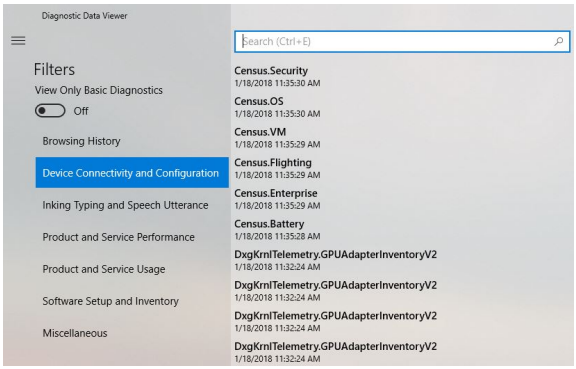
De *diagnostic data viewer* is een app[37] die een gebruiker (of beheerder) vanuit de windows store kan installeren op zijn device. Op dat device wordt dan worden bekeken en beoordeelt welke gegevens verzameld zijn/worden. Het inzien is alleen voor het device waarop de viewer is geïnstalleerd. Met de App kunnen de "JSON" bestanden worden gelezen.

Gezien het technische karakter van deze data viewer is het uitrollen hiervan voor alle gebruikers mogelijk niet optimaal. (zie afbeeldingen)



Figuur 1 The Diagnostic Data Viewer shows the exact details sent to Microsoft (bron microsoft)

[37] https://blogs.windows.com/windowsexperience/2018/01/24/microsoft-introduces-new-privacy-tools-ahead-of-data-privacy-day/



Figuur 2 The detailed menu, a list of diagnostic event categories (bron Microsoft)

8.4.2 Delete by device ID

De functie *delete by device ID* geeft eindgebruikers vanuit de Windows-instellingen de mogelijkheid om een instructie te geven aan Microsoft om alle verzamelde gegevens van het apparaat te verwijderen. Dit is een instelling binnen het privacy dashboard, binnen Windows instellingen. Het is niet duidelijk wat het geven van deze opdracht binnen een Enterprise omgeving voor gevolgen heeft anders dan dat gegevens die door Microsoft zijn opgeslagen in de VS zullen worden verwijderd. De functie heeft ook geen effect op toekomstige dataverzamelingen. De gebruiker zal deze functie periodiek moeten uitvoeren als actieve handeling. Door het uitvoeren van de functie wordt alleen een verwijderverzoek verstuurd; het verzamelen en verzenden van diagnostische data wordt er niet mee onderbroken of gestopt.

8.4.3 Configuratie-instellingen

Naast de hierboven beschreven nieuwe functies worden in een Enterprise omgeving drie specifieke configuratie-instellingen beschikbaar gesteld in de spring release (twee nieuwe, één reeds bestaande);

- **Allow Telemetry**: De policy setting waarmee het niveau van verzamelen van diagnostische data ingesteld kan worden.
- **Configure telemetry opt-in change notifications**: (nieuwe instelling) Door middel van deze setting kan worden bepaald of bij een eerste inlog van een gebruiker, of bij veranderingen in de configuratie, informatie getoond wordt die de gebruiker notificeert over het gebruik en verzamelen van telemetrie gegevens. Microsoft adviseert zelf om dit aan te zetten voor medewerkers binnen Europa.
- **Configure telemetry opt-in setting user interface**: (nieuwe instelling) Met behulp van deze instelling wordt bepaald of eindgebruikers zelf veranderingen kunnen aanbrengen in de niveau's van verzamelen van gegevens.

Microsoft geeft aan dat deze 'enterprise settings' haar rol als verwerkingsverantwoordelijke ondersteunen.

Er is voorzien dat in een latere release een centrale beoordeling van de "JSON" bestanden (de bestanden met de diagnostische en telemetrie data) mogelijk wordt gemaakt. Mede door de gebruikte cryptografische technieken (end to end SSL met certificate pinning) is het standaard niet mogelijk om in de gegevensstroom tussen Windows 10 station en Microsoft inhoudelijke details van de overdracht in te zien.

De nieuwe features van dit voorjaar zijn gericht op het vergroten van de transparantie en controle voor de gebruiker. Ze hebben geen invloed op de verwerking van telemetriegegevens als die eenmaal zijn verzameld door Microsoft.

9. Juridisch en beleidsmatig kader

We gaan hieronder achtereenvolgens in op de volgende zaken:

- de Europese gegevensbeschermingswetgeving, in het bijzonder de e-Privacyverordening;
- de eis van goed werkgeverschap;
- de overeenkomsten tussen het Rijk en Microsoft;
- Amerikaanse wetgeving over de toegang tot gegevens.
- het onderzoek van de AP.

9.1 Europese gegevensbeschermingswetgeving

Vanaf 25 mei 2018 is de AVG van toepassing op de verwerking van telemetriegegevens van medewerkers van Nederlandse overheidsinstanties door Microsoft. (En voor de periode daarvoor heeft Microsoft zich ertoe verplicht om de Europese privacyregels na te leven. [38])

De telemetriegegevens worden immers door Microsoft Corp. verwerkt "in het kader van de activiteiten van haar vestiging Microsoft Ierland" (art. 3(1) AVG), omdat de verwerking van de telemetriegegevens zonder de overeenkomst tussen JenV en Microsoft Ierland niet zou bestaan. Ten opzichte van de huidige Wet bescherming persoonsgegevens (Wbp) scherpt de AVG vooral de rechten van de betrokkene aan (waaronder de transparantie jegens de gebruikers) alsmede de verplichtingen van de verantwoordelijke (in casu Microsoft Corp) om aantoonbaar aan de AVG te voldoen.

9.1.1 e-Privacyverordening

In 2019, of mogelijk 2020, gaat de e-Privacyverordening (hierna: ePV) de bepalingen van hoofdstuk 11 Telecommunicatiewet vervangen. Daarmee wordt in Europa één regime geïntroduceerd met betrekking tot privacy in elektronische diensten.

De ePV is momenteel nog volop in onderhandeling in Brussel. In onderstaande gaan wij uit van de teksten zoals die door het Europees Parlement zijn vastgesteld in haar 'eerste lezing'.[39]

[38] "Microsoft zal zich houden aan de vereisten van de wetgeving inzake bescherming van persoonsgegevens van de Europese Economische Ruimte en Zwitserland betreffende het verzamelen, gebruiken, overdragen, bewaren en op overige wijze verwerken van persoonsgegevens uit de Europese Economische Ruimte en Zwitserland."

[39] De Raad heeft nog geen gemeenschappelijke positie bepaald, zodat het lastig is om uitspraken te doen over de stukken die uit de Raad komen.

Van de e-Privacy verordening is met name de onderstaande bepaling van belang. N.B. De wijzigingsvoorstellen van het Parlement ten opzichte van het voorstel van de Europese Commissie zijn vetgedrukt.

Artikel 8 lid 1 e-Privacyverordening

*The use of processing and storage capabilities of terminal equipment and the collection of information from **end-users'** terminal equipment, including about its software and hardware, other than by the **user** concerned shall be prohibited, except on the following grounds:*

*(a) it is **strictly** necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or*
*(b) the **user** has given his or her **specific** consent; or*
*(c) it is **strictly technically** necessary for providing an information society service **specifically** requested by the user; or*
*(d) if it is **technically** necessary for measuring **the reach of an information society service requested by the user**, provided that such measurement is carried out by the provider, **or on behalf** of the **provider**, or **by a web analytics agency acting in the public interest including for scientific purpose; that the data is aggregated and the user is given a possibility to object; and further provided that no personal data is made accessible to any third party and that such measurement does not adversely affect the fundamental rights of the user; Where audience measuring takes place on behalf of an information society service provider, the data collected shall be processed only for that provider and shall be kept separate from the data collected in the course of audience measuring on behalf of other providers**; or*

(da) it is necessary to ensure security, confidentiality, integrity, availability and authenticity of the terminal equipment of the end-user, by means of updates, for the duration necessary for that purpose, provided that:
(i) this does not in any way change the functionality of the hardware or software or the privacy settings chosen by the user;
(ii) the user is informed in advance each time an update is being installed; and
(iii) the user has the possibility to postpone or turn off the automatic installation of these updates;
(db) in the context of employment relationships, it is strictly technically necessary for the execution of an employee's task, where:
(i) the employer provides and/or is the user of the terminal equipment;
(ii) the employee is the user of the terminal equipment; and
(iii) it is not further used for monitoring the employee.

9.1.2 Telecommunicatiewet

Zolang de ePV nog niet van toepassing is, geldt de e-Privacy richtlijn zoals geïmplementeerd in hoofstuk 11 Telecommunicatiewet (Tw). Voor telemetriegegevens is artikel 11.7a Tw relevant (ook wel bekend als de 'cookiewet'). De relevante onderdelen daarvan zijn hieronder weergegeven.

Artikel 11.7a Telecommunicatiewet

1. Onverminderd de Wet bescherming persoonsgegevens is het via een elektronisch communicatienetwerk opslaan van of toegang verkrijgen tot informatie in de randapparatuur van een gebruiker, alleen toegestaan op voorwaarde dat de betrokken gebruiker:

a. is voorzien van duidelijke en volledige informatie overeenkomstig de Wet bescherming persoonsgegevens, in ieder geval over de doeleinden waarvoor deze informatie wordt gebruikt, en

b. daarvoor toestemming heeft verleend.

[…]

3. Het bepaalde in het eerste lid is niet van toepassing indien het de opslag of toegang betreft:

a. met als uitsluitend doel de communicatie over een elektronisch communicatienetwerk uit te voeren,

b. die strikt noodzakelijk is om de door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij te leveren of – mits dit geen of geringe gevolgen heeft voor de persoonlijke levenssfeer van de betrokken abonnee of gebruiker – om informatie te verkrijgen over de kwaliteit of effectiviteit van een geleverde dienst van de informatiemaatschappij.

[…]

Of de verwerking van telemetriegegevens door Microsoft aan dit artikel voldoet, bespreken we in paragraaf 11.

9.2 Goed werkgeverschap

Van een werkgever wordt verwacht dat hij zich gedraagt als goed werkgever[40]. Belangrijk onderdeel van het goed werkgeverschap is de zorgvuldigheidsnorm; dat houdt in dat de werkgever bij zijn handelen de wederzijds betrokken belangen zorgvuldig tegen elkaar dient af te wegen. Een werkgever mag geen inbreuk maken op de privacy van de werknemer tenzij het belang van de onderneming dat onvermijdelijk maakt[41]. Dit betekent ook dat een werkgever bij de inkoop van diensten rekening dient te houden met de privacybelangen van zijn werknemers, ook als onder de Wbp/AVG de dienstverlener voor de gegevensverwerking de verantwoordelijke is. Het feit dat de werkgever geen verantwoordelijke is voor de gegevensverwerking, ontslaat hem niet van de verplichting om alleen zaken te doen met partijen die netjes met de gegevens van zijn medewerkers omgaan. Er is immers sprake van 'gedwongen winkelnering' omdat de werknemers geen andere keus hebben.

9.3 Overeenkomsten tussen het Rijk en Microsoft

De contractuele structuur bestaat uit de volgende documenten:

- Microsoft Business and Services Agreement (MBSA);
- Amendment ID CTM van het MBSA;
- De Microsoft Voorwaarden voor Online Diensten.

[40] Artikel 7:611 Burgerlijk Wetboek

[41] G.J.J. Heerma Van Voss¸ Goed werkgeverschap als bron van vernieuwing van het arbeidsrecht, 1993, p. 85

9.3.1 Amendment ID CTM van het MBSA

Het Amendment ID CTM is een overeenkomst tussen Microsoft Ireland Operations Limited en de Staat der Nederlanden, daarbij vertegenwoordigd door de Minister van Veiligheid en Justitie, ten behoeve van alle Gelieerde Ondernemingen.

Dit document bevat enkele afwijkingen/wijzigingen van de Microsoft Business and Services Agreement (MBSA). De voor deze DPIA belangrijkste wijziging is de definitie van het begrip "Gegevens van de Klant", te weten: alle gegevens, met inbegrip van alle tekst-, geluids-, software-, beeld-, of videobestanden, die aan Microsoft zijn gegeven door, of namens, de Klant en zijn Gelieerde Ondernemingen door middel van het gebruik van de Online Diensten of via de Professionele Diensten. De telemetriegegevens vallen echter niet onder deze definitie, omdat die gegeven niet door de klant aan Microsoft worden "gegeven", maar over de medewerker van de klant worden verzameld door Microsoft.

Verder is er een bepaling opgenomen voor de overgang van de Wet bescherming persoonsgegevens naar de AVG, die erop neerkomt dat Microsoft de klant zo spoedig mogelijk zal informeren over de wijze waarop Microsoft de AVG zal naleven.

9.3.2 Microsoft Business and Services Agreement (MBSA)

Het Microsoft Business and Services Agreement (MBSA) bevat de belangrijkste voorwaarden waaronder Microsoft de diensten levert. Belangrijke aandachtspunten zijn:

1) Op de MBSA is het recht van Nederland van toepassing. Dit betekent dat de uitleg van de overeenkomst geschiedt naar Nederlands recht c.q. de AVG.

2) De MBSA laat het toe dat Microsoft Ierland gegevens laat verwerken door andere Microsoft-ondernemingen. Voor zover deze buiten de EU gevestigd zijn, zijn de Europese Standaardcontractsclausules van toepassing (opgenomen in Bijlage 3 VOD, zie hierna). Echter, deze bepaling ziet niet op de verwerking van de telemetriegegevens door Microsoft Corp. Ten eerste is Microsoft Corp voor de verwerking van telemetriegegevens geen verwerker van Microsoft Ierland, maar zelf een verantwoordelijke. En ten tweede is er geen sprake van internationaal gegevensverkeer als bedoeld in hoofdstuk 5 AVG omdat Microsoft Corp. zich op grond van artikel 3(1) AVG al aan de AVG moet houden.[42]

9.3.3 Voorwaarden voor Online Diensten

Het document Voorwaarden voor Online Diensten (1 februari 2018) bevat de algemene voorwaarden voor de Microsoft enterprise clouddiensten. Van dit document zijn een tweetal paragrafen relevant:

1) Voorwaarden voor privacy en beveiliging. Deze paragraaf bevat samen met Bijlage 4 de voorwaarden zoals gesteld wordt door artikel 14 Wbp/28 AVG (de verwerkersovereenkomst). Die bepalingen gelden voor alle Online Diensten, met uitzondering van een aantal diensten die hun eigen voorwaarden hebben (en waarvoor Microsoft een verwerkingsverantwoordelijke is). De privacyparagraaf in de VOD bevat een groot aantal bepalingen die gangbaar zijn voor verwerkersovereenkomsten zoals een beperking van het gebruik van de gegevens, een verbod op het verstrekken van gegevens aan derden (tenzij dit door de klant wordt verlangd, het gevolg is van de Online Diensten, dan wel in geval van een wettelijke verplichting, een verplichting om de

[42] Naar zowel het systeen van de AVG als de bedoeling van hoofdstuk 5 AVG, is hoofdstuk 5 alleen relevant als er een Europese 'data exporteur' is die zich aan de AVG moet houden en een niet-Europese data importeur die zich niet rechtstreeks aan de AVG moet houden, maar die via bijv. de Standaardcontractsclausules vergelijkbare verplichtingen krijgt opgelegd

gegevens te beveiligen, een meldplicht datalekken bij de klant, een regeling inzake de plaats van de gegevensverwerking en de eventuele mogelijkheid van internationaal gegevensverkeer, een regeling voor het inschakelen van subverwerker, het teruggeven van de gegevens aan de klant, alsmede medewerkingsverplichtingen bij de uitoefening van rechten van betrokkenen. Daarnaast bevat de VOD een aantal bepalingen zien op compliance met het buitenlandse recht en die voor de Nederlandse situatie dus niet relevant zijn (bijv. Zakenpartner HIPAA). Voor compliance met de AVG is Bijlage 4 van toepassing. Bijlage 4 volgt nauwkeurig de eisen zoals gesteld door artikel 28 AVG (verwerkersovereenkomst) en artikel 32 AVG (beveiliging) en geldt pas vanaf 25 mei 2018. Bijlage 4 is relevant voor de gegevens die op de servers van Microsoft Ierland zijn opgeslagen, maar is niet van toepassing op de telemetriegegevens, omdat Microsoft voor die laatste de verwerkingsverantwoordelijke is.

2) Bijlage 3, de Standaardcontractsclausules voor verwerkers. Deze bijlage bevat de regeling voor een eventuele gegevensdoorgifte tussen de klant en Microsoft Corporation en is alleen relevant voor zover Microsoft Corp. optreedt als verwerker voor de klant. In principe is daar geen sprake van in geval de gegevens bij Microsoft Ierland worden opgeslagen, noch in geval van de telemetriegegevens.

N.B. Wij merken op dat geen van de contractsdocumenten iets zegt over de telemetriegegevens. Derhalve kunnen in ieder geval contractuele vraagtekens worden gezet bij de bevoegdheid van Microsoft Corp. om de telemetriegegevens te verzamelen.

9.4 Amerikaanse wetgeving

Indirect is ook de Amerikaanse wetgeving op het gebied van de toegang tot en het vorderen van gegevens van belang. Deze hebben wij uitgewerkt in bijlage 5.

9.5 Onderzoek AP

In oktober 2017 heeft de AP geconstateerd dat Microsoft bij het verzamelen van telemetriegegevens in Windows 10 Home en Pro in strijd handelt met de Wet bescherming persoonsgegevens en de telecommunicatiewet. Door de werkwijze van Microsoft hebben de gebruikers volgens de AP gebrek aan controle over hun gegevens. Ze weten niet welke gegevens waarvoor worden gebruikt, noch dat er op basis van deze gegevens gepersonaliseerde advertenties en aanbevelingen aan hen kunnen worden getoond, als de gebruikers dit bij installatie, of daarna, niet hebben uitgeschakeld. Op 5 april heeft de AP in een persbericht laten weten dat Microsoft in de April-update van Windows 10 de overtredingen zal beëindigen. Zo informeert Microsoft gebruikers beter over de gegevens die door Microsoft worden verzameld en over de doeleinden waarvoor deze worden verwerkt. Daarnaast kunnen gebruikers op een duidelijke actieve wijze kiezen voor hun privacy-instellingen. Uit het bericht blijkt niet of dit ook gaat gelden voor de Enterprise-versie.

10. Bewaartermijnen

Microsoft zegt over het bewaren van telemetriegegevens het volgende:[43]

> ***Retention***
>
> *Microsoft believes in and practices information minimization. We strive to gather only the info we need and to store it only for as long as it's needed to provide a service or for analysis. Much of the info about how Windows and apps are functioning is deleted within 30 days. Other info may be retained longer, such as error reporting data or Microsoft Store purchase history.*

Microsoft hanteert voor telemetriegegevens als uitgangspunt een bewaartermijn van 30 dagen. Dat lijkt in algemene zin niet onredelijk, mede gelet op het principe van dataminimalisatie dat Microsoft zegt te hanteren. Een en ander is echter niet goed specifiek te beoordelen, aangezien niet duidelijk is voor welke doeleinden bewaarde gegevens (nog) gebruikt kunnen worden. In sommige gevallen kunnen gegevens bovendien ook langer bewaard worden. Niet duidelijk is in welke gevallen precies, en evenmin hoeveel langer gegevens in die gevallen bewaard kunnen worden. Tot slot is de vraag of verwijderen ("delete") hier gelezen kan worden als wissing ("erasure") in de zin van art. 17 AVG.

B. Beoordeling rechtmatigheid gegevensverwerkingen

Inleiding bij Deel B

In dit deel beoordelen we de rechtmatigheid van de verwerking van telemetriegegevens. Daarbij is het volgende van belang. Normaliter wordt een DPIA uitgevoerd door de verwerkingsverantwoordelijke.[44] Bij deze DPIA ligt dat anders. Zoals we hebben uiteengezet in paragraaf 5 en bijlage 1 is weliswaar Microsoft de belangrijkste verwerkingsverantwoordelijke voor telemetrie, maar is voor elke specifieke toepassing van telemetrie bij een overheidsinstantie die overheidsinstantie medeverantwoordelijke (gezamenlijke verantwoordelijkheid).

Dit heeft gevolgen voor de insteek van de beantwoording van de vragen in dit deel. Het is immers onmogelijk om "vanaf de zijlijn" een diepgravende analyse en beoordeling te doen van de overwegingen en belangen die hier spelen. Dat is zoals gezegd aan de verwerkingsverantwoordelijke zelf. Microsoft heeft aangegeven op dit moment zelf een DPIA uit te voeren op de verwerking van telemetriegegevens. Het heeft aangegeven niet voornemens te zijn om de volledige DPIA-rapportage met de buitenwereld te delen, maar wel de informatie over de uitkomsten van de DPIA beschikbaar te zullen stellen die noodzakelijk is voor klanten met het oog op hun eigen AVG-compliance. Door deze informatie kritisch te beoordelen kan de overheid zich een beeld vormen of Microsoft voldoende kan onderbouwen dat de wijze waarop telemetrie is vormgegeven slechts gegevensverwerking met zich meebrengt die noodzakelijk is om haar gerechtvaardigde belangen te dienen. Daarbij kan zij uiteraard gebruik maken van andere informatie die bij die beoordeling behulpzaam kan zijn. In dit geval gaat het dan met name om de

[43] https://docs.microsoft.com/nl-nl/windows/configuration/configure-windows-diagnostic-data-in-your-organization.
[44] En soms ook door een verwerker, ter ondersteuning van een DPIA op het gebruik van zijn systeem door klanten.

uitkomsten van het onderzoek dat de AP heeft uitgevoerd naar telemetrie in Windows 10 Home en Pro. Complicerende factor bij dat laatste, is dat de AP in een bericht van 5 april heeft aangegeven dat Microsoft nog diezelfde maand een update zal doorvoeren waarmee het de geconstateerde overtredingen beëindigt. De AP geeft echter geen details. Dat maakt het onmogelijk om de doorgevoerde wijzigingen goed te beoordelen; in het bijzonder is niet vast te stellen in hoeverre de conclusies van de AP overdraagbaar zijn naar Windows 10 Enterprise.

Het is tegen deze achtergrond dat wij de onderstaande paragrafen hebben geschreven, gebaseerd op de momenteel beschikbare informatie.

11. Rechtsgrond

In deze paragraaf gaan we kort in op de rechtsgrond voor de verwerking van telemetriegegevens door Microsoft. Die heeft het nodig op grond van art. 6 lid 1 AVG.

In aanvulling hierop zijn er enkele andere aspecten die raken aan de rechtmatigheid van de verwerking en voor de beoordeling waarvan het gehanteerde model geen natuurlijke plek biedt om die te bespreken. We hebben er daarom voor gekozen om ook die aspecten in deze paragraaf aan bod te laten komen.

In de eerste plaats gaat het dan over de invloed die de overheidsinstantie uitoefent op de verwerking van telemetriegegevens. Zij verwerkt bij telemetrie zelf geen persoonsgegevens, en heeft daarom geen formele rechtsgrond nodig. Maar wel dient zij vanuit het oogpunt van behoorlijke gegevensverwerking (art. 5 lid 1 onder a AVG) de keuze voor een bepaald niveau van telemetrie te kunnen onderbouwen.

Meer aandacht verdient de vraag in hoeverre de verwerking van telemetriegegevens is toegestaan op grond van de Telecommunicatiewet, en zal zijn toegestaan als die over enige tijd is vervangen door de e-Privacyverordening.

11.1 Rechtsgrond Microsoft

Artikel 6 lid 1 AVG somt zes rechtsgronden op waarop een verwerking van persoonsgegevens gestoeld kan zijn. A priori zouden hiervan toestemming, een overeenkomst of het gerechtvaardigd belang in aanmerking kunnen komen. Om dezelfde redenen als die we hieronder in het deel over de Telecommunicatiewet en de e-Privacyverordening uiteenzetten, komt toestemming in de onderhavige context niet in aanmerking. Ook kan de verwerking niet op een overeenkomst gebaseerd worden, aangezien Microsoft geen overeenkomst heeft met de betrokkenen.

De enig mogelijke rechtsgrond die resteert, is dan dat de verwerking van telemetriegegevens noodzakelijk is voor een gerechtvaardigd belang van Microsoft, dat bovendien zwaarder weegt dan de belangen en rechten van degenen over wie telemetriegegevens worden verzameld.

Wanneer we kijken naar de doeleinden en belangen van Microsoft, zoals die uiteen zijn gezet in de paragrafen 4 en 6, dan zijn we van oordeel dat het hier gaat om gerechtvaardigde belangen.

Het is echter bijzonder lastig, zeker vanaf de buitenkant, om te beoordelen in hoeverre de verwerking van telemetriegegevens zoals die nu is ingericht ook noodzakelijk is (d.w.z. voldoet aan de vereisten van proportionaliteit en subsidiariteit) met het oog op die belangen. En aanvullend daarop: hoe ruim kan een belang gedefinieerd of geïnterpreteerd worden om toch nog als "gerechtvaardigd" beschouwd te kunnen blijven worden? Zoals in de inleiding hierboven aangegeven is het primair aan Microsoft als primaire (mede-)verwerkingsverantwoordelijke om deze afwegingen te maken. Deze vragen gelden voor telemetrie in het algemeen, en in het

bijzonder waar daarbij sprake is van (semi-)geautomatiseerde besluitvorming, profilering of big-data verwerkingen.

Voor de afweging van de belangen van Microsoft tegen die van de betrokkenen gelden vergelijkbare overwegingen. Wel kan de overheid op dat punt meer geïnformeerd een standpunt innemen. Zij kent immers beter dan Microsoft de belangen van de betrokkenen in deze specifieke context. Onderdeel C van de definitieve versie van dit rapport zal daarvoor ook input leveren.

Van belang zijn hier verder de bevindingen van de AP in haar onderzoek naar Windows 10 Home en Pro. De AP erkent de belangen van Microsoft bij telemetrie, maar komt niettemin tot de conclusie dat zij de verwerking van telemetriegegevens niet kan baseren op haar gerechtvaardigd belang. De argumenten daarvoor zijn met name dat Microsoft onvoldoende onderscheid maakt naar de verschillende doeleinden van telemetrie, terwijl voor enkele van die doeleinden telemetrie niet noodzakelijk is; en dat Microsoft gegevens van gevoelige aard verwerkt, zoals bezochte URL's, gebruikte apps en ingevoerde locatie, die principieel vertrouwelijk dienen te blijven. Uit de beschikbare informatie blijkt op geen enkele wijze dat dit voor Windows 10 Enterprise anders zou liggen. Blijkens het bericht van de AP van 5 april worden Windows 10 Home en Pro ook op dit punt compliant met de update van dit voorjaar. En ook hiervoor geldt dat het bij gebrek aan nadere details onmogelijk is om te beoordelen in hoeverre de doorgevoerde wijzigingen ook van toepassing zijn voor Windows 10 Enterprise, en zo ja, of ze ook een eventueel probleem met Windows 10 Enterprise op dit vlak zouden verhelpen.

Voor een individuele overheidsinstantie is het uiteraard lastig om te beoordelen, zelfs marginaal, in hoeverre de gegevensverwerking door Microsoft een rechtsgrond kent en ook in overige opzichten aan de AVG voldoet. Het ligt daarom voor de hand dat DI&I dit oppakt voor zover het nadere beoordeling hiervan aangewezen acht.

11.2 Keuze telemetrieniveau door overheidsinstantie

De overheidsinstantie heeft een kleine maar belangrijke rol als mede-verwerkingsverantwoordelijke. Zij bepaalt immers welke mate van telemetrie zij toestaat aan Microsoft. Zoals we in paragraaf 6 hebben aangegeven, ziet zij zich daarbij geconfronteerd met tegengestelde belangen. Enerzijds heeft zij er belang bij dat haar medewerkers kunnen werken met de gangbare software van Microsoft. Anderzijds dient zij zich richting haar werknemers als goed werkgever te gedragen.

Wanneer we kijken naar de verschillende niveaus van telemetrie, dan is het toestaan van telemetrie op het niveau Security goed te onderbouwen. Zoals is uitgewerkt in paragraaf 16 zijn de privacyrisico's voor de werknemer op dit niveau beperkt. Bovendien is telemetrie op niveau Security noodzakelijk om Microsoft in staat te stellen om essentiële beveiligingsfunctionaliteit te leveren. Die functionaliteit helpt voorkomen dat de gebruiker van het apparaat slachtoffer wordt van diefstal van gegevens op het apparaat, waaronder zijn persoonsgegevens. Daarmee beoordelen wij, binnen de beoordelingscontext van deze DPIA, de privacyvoordelen van telemetrie op niveau Security hoger dan de privacyrisico's ervan.[45]

Van de andere kant is niet goed in te zien waarom een doorsnee overheidsinstantie telemetrie op niveau Basic of hoger zou toestaan. Het gaat daarbij namelijk om verwerking van gegevens van medewerkers waar noch de medewerkers noch de overheidsinstantie zelf direct belang bij heeft.

---

[45] Het is mogelijk om voor een deel van de genoemde beveiligingsfunctionaliteit software van andere leveranciers te gebruiken. Dat betekent echter extra investeringen, terwijl niet gezegd is dat de privacyrisico's daarmee lager worden: dat hangt af van hoe de betreffende leveranciers hun gegevensverwerking hebben ingericht. Niettemin kan dit vanuit het oogpunt van het beperken van leveranciersafhankelijkheid een interessante optie zijn. Telemetrie helemaal uitzetten is vanuit beveiligingsoogpunt sterk af te raden, omdat dan bijv. ook essentiële informatie over bijv. veiligheidscertificaten niet beschikbaar is.

Microsoft heeft aangegeven dat alle essentiële functionaliteit, waaronder Office, probleemloos werkt op niveau Security. Telemetrie vanaf het niveau Basic dient vooral de belangen van Microsoft. Het getuigt dan zonder goede onderbouwing niet van goed werkgeverschap om werknemers deze verwerking van hun gegevens op te leggen.

We concluderen dat voor overheidsinstanties in het algemeen telemetrie op niveau Security aangewezen is.

Zoals in paragraaf 2.2.5 is aangegeven, is het mogelijk om met een grotere mate van detail de doorgifte van specifieke telemetriegegevens aan of uit te zetten. Een overheidsinstantie kan er uiteraard voor kiezen om op basis van een aanvullende risicoanalyse zulke aanvullende keuzes te maken: ofwel de overdracht van bepaalde gegevens op niveau Security uitzetten, ofwel de overdracht van bepaalde gegevens aanvullend op niveau Security aanzetten. Daarbij moet zij wel rekening houden met de risico's die de daarmee gepaard gaande extra complexiteit en beheer last met zich meebrengen. Om die reden bevelen wij de keuze voor niveau Security aan.

11.3 Telecommunicatiewet en e-Privacyverordening

Hieronder analyseren we in hoeverre de verwerking van telemetriegegevens door Microsoft is toegestaan onder de huidige Telecommunicatiewet, en ook onder de e-Privacyverordening, wanneer die in werking is getreden.

De conclusies luiden in essentie als volgt:

- Telecommunicatiewet
  - telemetrie is toegestaan indien en voor zover
    - telemetrie strikt noodzakelijk is om een gevraagde dienst te leveren, of
    - telemetrie strikt noodzakelijk is om informatie te krijgen over de kwaliteit of effectiviteit van de geleverde dienst, en de privacygevolgen voor de werknemers klein of afwezig zijn;
  - De beoordeling of hieraan voldaan is, is primair aan Microsoft (als verwerkingsverantwoordelijke).
- e-Privacyverordening (N.B. huidige tekst, wordt nog over onderhandeld!)
  - telemetrie is niet toegestaan

11.3.1 Telecommunicatiewet

Op het opslaan van of toegang verkrijgen tot informatie in de randapparatuur van een gebruiker is artikel 11.7a Tw van toepassing.[46]

De relevante onderdelen daarvan zijn hieronder voor de overzichtelijkheid nogmaals weergegeven.

[46] Zie paragraaf 9.

Artikel 11.7a Tw
1. Onverminderd de Wet bescherming persoonsgegevens is het via een elektronisch communicatienetwerk opslaan van of toegang verkrijgen tot informatie in de randapparatuur van een gebruiker, alleen toegestaan op voorwaarde dat de betrokken gebruiker:
a. is voorzien van duidelijke en volledige informatie overeenkomstig de Wet bescherming persoonsgegevens, in ieder geval over de doeleinden waarvoor deze informatie wordt gebruikt, en
b. daarvoor toestemming heeft verleend.
[…]
3. Het bepaalde in het eerste lid is niet van toepassing indien het de opslag of toegang betreft:
a. met als uitsluitend doel de communicatie over een elektronisch communicatienetwerk uit te voeren,
b. die strikt noodzakelijk is om de door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij te leveren of – mits dit geen of geringe gevolgen heeft voor de persoonlijke levenssfeer van de betrokken abonnee of gebruiker – om informatie te verkrijgen over de kwaliteit of effectiviteit van een geleverde dienst van de informatiemaatschappij.
[…]

Zoals is aangegeven in paragraaf 6 zal de overheidsinstantie de werknemer geen keuze willen laten met betrekking tot het al dan niet laten verwerken van bepaalde telemetriegegevens. Daar komt nog bij dat mocht de werknemer wel een keuze hebben, het in het kader van de arbeidsrelatie zo goed als uitgesloten is dat deze zou voldoen aan de eisen die de AVG stelt aan toestemming als rechtsgrond voor gegevensverwerking.[47] Met andere woorden, Microsoft kan zich niet beroepen op het eerste lid van artikel 11.7a.

De vraag is daarmee in hoeverre de verwerking van telemetriegegevens valt onder de uitzondering in het derde lid. In de eerste plaats kan men zich de vraag stellen hoe ruim de voorwaarde uit onderdeel a "met als uitsluitend doel de communicatie over een elektronisch communicatienetwerk uit te voeren" begrepen moet worden. Uit het onderzoeksrapport van de AP blijkt impliciet dat de AP van mening is dat het verzamelen van telemetriegegevens hieronder valt. Wij sluiten ons hierbij aan.

Omdat het niveau van de telemetriegegevens door de overheidsinstantie wordt bepaald, kan er ook geen sprake zijn van een grondslag op basis van de eerst genoemde mogelijkheid in het derde lid onder (b). Dat zou anders kunnen liggen als – wat echter momenteel niet het geval is – de telemetriegegevens op niveau Security uitsluitend gebruikt zouden worden voor het laten functioneren van Windows Defender en de Malicious Software Removal Tool.

Resteert de tweede mogelijkheid in het derde lid onder (b). Vraag is dan in hoeverre telemetrie voldoet aan de daar gestelde eisen. Dat is het geval als aan beide volgende eisen is voldaan:
- telemetrie is strikt noodzakelijk om informatie te krijgen over de kwaliteit of effectiviteit van de geleverde dienst;
- de privacygevolgen voor de werknemers zijn klein of afwezig.

[47] Vgl. overweging 43 van de AVG: "Om ervoor te zorgen dat toestemming vrijelijk wordt verleend, mag toestemming geen geldige rechtsgrond zijn voor de verwerking van persoonsgegevens in een specifiek geval wanneer er sprake is van een duidelijke wanverhouding tussen de betrokkene en de verwerkingsverantwoordelijke, met name wanneer de verwerkingsverantwoordelijke een overheidsinstantie is, en dit het onwaarschijnlijk maakt dat de toestemming in alle omstandigheden van die specifieke situatie vrijelijk is verleend."

De beoordeling of hieraan voldaan is, is primair aan Microsoft (als verwerkingsverantwoordelijke).

11.3.2 e-Privacyverordening

In 2019, of mogelijk 2020, gaat de e-Privacyverordening (hierna: ePV) de bepalingen van hoofdstuk 11 Telecommunicatiewet vervangen.

De relevante onderdelen daarvan zijn hieronder voor de overzichtelijkheid nogmaals weergegeven.

Artikel 8 lid 1 e-Privacyverordening

*The use of processing and storage capabilities of terminal equipment and the collection of information from **end-users'** terminal equipment, including about its software and hardware, other than by the **user** concerned shall be prohibited, except on the following grounds:*

*(a) it is **strictly** necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or*
*(b) the **user** has given his or her **specific** consent; or*
*(c) it is **strictly technically** necessary for providing an information society service **specifically** requested by the user; or*
*(d) if it is **technically** necessary for measuring **the reach of an information society service requested by the user**, provided that such measurement is carried out by the provider, **or on behalf** of the **provider**, or **by a web analytics agency acting in the public interest including for scientific purpose; that the data is aggregated and the user is given a possibility to object; and further provided that no personal data is made accessible to any third party and that such measurement does not adversely affect the fundamental rights of the user; Where audience measuring takes place on behalf of an information society service provider, the data collected shall be processed only for that provider and shall be kept separate from the data collected in the course of audience measuring on behalf of other providers**; or*

(da) it is necessary to ensure security, confidentiality, integrity, availability and authenticity of the terminal equipment of the end-user, by means of updates, for the duration necessary for that purpose, provided that:

(iv) this does not in any way change the functionality of the hardware or software or the privacy settings chosen by the user;
(v) the user is informed in advance each time an update is being installed; and
(vi) the user has the possibility to postpone or turn off the automatic installation of these updates;

(db) in the context of employment relationships, it is strictly technically necessary for the execution of an employee's task, where:

(iv) the employer provides and/or is the user of the terminal equipment;
(v) the employee is the user of the terminal equipment; and
(vi) it is not further used for monitoring the employee.

Bij het verwerken van telemetriegegevens is de reden onder (a) niet van toepassing, en die onder (da) slechts zeer beperkt. Dit houdt in dat telemetriegegevens in het algemeen alleen verwerkt kunnen worden:

- met toestemming van de gebruiker, ofwel de werknemer;
- voor zover dat noodzakelijk is om de door de werknemer aangevraagde dienst aan te bieden; dan wel
- in het kader van de arbeidsrelatie voor zover dit vanuit technisch oogpunt strikt nodig is voor de uitoefening van de taken van de werkgever.

Om vergelijkbare redenen als hierboven uiteengezet ten aanzien van de Tw komt toestemming (b) niet als grondslag in aanmerking.

Omdat het niveau van de telemetriegegevens door de overheidsinstantie wordt bepaald, kan er ook geen sprake zijn een grondslag onder (c). Net zoals bij de Telecommunicatiewet zou dat anders kunnen liggen als – wat echter momenteel niet het geval is – de telemetriegegevens op niveau Security uitsluitend gebruikt zouden worden voor het laten functioneren van Windows Defender en de Malicious Software Removal Tool. Complicatie daarbij in vergelijking met de Tw kan dan wel zijn dat in de ePV de dienst moet zijn aangevraagd door de werknemer: er valt over te twisten of het de werkgever of de werknemer is die de dienst aanvraagt.

Afhankelijk van de inhoud van de verzamelde telemetriegegevens komt wellicht de grondslag onder (d) in aanmerking. Daar zitten echter allerlei voorwaarden aan, die in een situatie waarin werknemers gebruik maken van een door hun werkgever ingekochte dienst, lastig zijn te implementeren. De opdrachtgever heeft aangegeven dat overheidsinstanties in de praktijk de werknemers de mogelijkheid zal willen ontnemen om zelf invloed uit te oefenen op de verwerking van de telemetriegegevens. In dat geval is deze grondslag niet van toepassing.

Uitzondering (db), zoals voorgesteld door het Europees Parlement, is wel een mogelijke grondslag voor het verzamelen van telemetriegegevens, mits aan deze beide voorwaarden is voldaan:

- de telemetriegegevens worden verzameld in het belang van de werkgever (en dus niet uitsluitend in het belang van Microsoft), in die zin dat de werknemer anders zijn taken niet kan uitvoeren;
- de werkgever gebruikt de gegevens niet voor het monitoren van de medewerker, zoals diens aanwezigheid, gedrag of prestaties (vergelijk art. 27 lid 1 sub L Wet op de ondernemingsraden). Met andere woorden, de telemetriegegevens mogen niet worden gebruikt als personeelsvolgsysteem.

Voor de meeste bij telemetrie verwerkte gegevens geldt dat verwerking ervan niet noodzakelijk is om de werknemer zijn taken te kunnen laten uitvoeren.

We concluderen dat de huidige tekst van de ePV geen basis biedt voor de verwerking van telemetriegegevens. Met andere woorden: als de tekst van de ePV blijft zoals die nu is, dan zal Microsoft zodra de ePV van kracht wordt moeten ophouden met het toepassen van alle telemetrie die niet als doel heeft om de medewerkers van de overheidsinstantie in staat te stellen om hun taken uit te voeren.

12. Bijzondere persoonsgegevens

Microsoft geeft aan het verwerken van bijzondere gegevens bij telemetrie zoveel mogelijk te vermijden. Helemaal te vermijden is het echter niet, aangezien bijvoorbeeld crash dumps delen van gebruikersbestanden kunnen bevatten. Naar de letter van de wet heeft Microsoft daarmee een probleem: geen van de uitzonderingen op het verwerkingsverbod van bijzondere gegevens is hier van toepassing.

De vraag is echter of hier ook daadwerkelijk sprake is van een onoverkomelijke belemmering. Het is namelijk niet onwaarschijnlijk dat in ieder geval rechters, en waarschijnlijk ook toezichthouders, hier een doelredenering zullern volgen: "het staat er wel, maar dit kan nooit de bedoeling geweest zijn". Een Nederlandse rechter heeft onlangs een dergelijke redenering gevolgd.[48] Het ging in die

[48] ECLI:NL:RBAMS:2018:1644. "4.8. In het verweer van Google ligt mede besloten dat zij zich erop beroept dat artikel 16 Wbp, waarmee de Privacy Richtlijn is geïmplementeerd, niet dient te gelden in het geval van het beschikbaar maken voor het publiek door een zoekmachine van publicaties waarin wordt bericht over strafrechtelijke persoonsgegevens betreffende medeburgers.

zaak over het verwerken van bijzondere persoonsgegevens door zoekmachines. De rechter stelde onder meer vast dat een uitzondering op het verwerkingsverbod formeel weliswaar ontbrak, maar dat een dergelijke strikte uitleg het functioneren van zoekmachines onmogelijk zou maken, terwijl zij een essentiële rol spelen bij het ontsluiten van informatie op internet. Een vergelijkbare aanpak is gevolgd door het Europese Hof van Justitie in de Lindqvist-zaak: formeel gezien is de publicatie van persoonsgegevens op internet wellicht te beschouwen als een doorgifte naar derde landen, maar het volgen van die lijn zou het publiceren van persoonsgegevens op internet effectief onmogelijk maken. Tekenend is in dit verband ook dat de AP in haar onderzoek genoegen neemt met de verzekering van Microsoft dat het zijn best doet om de verwerking van bijzondere gegevens zoveel mogelijk te beperken.

Wij concluderen dat er in het algemeen naar verwachting geen probleem zal zijn met het verwerken van bijzondere gegevens bij telemetrie, zolang dat werkelijk onvermijdelijk is. Aandachtspunt hierbij is nog dat sommige systeemkenmerken weliswaar worden verzameld ten behoeve van de algemene telemetriedoeleinden, maar naar hun aard niettemin bijzonder kunnen zijn. Wij denken hier met name aan gegevens over toegankelijkheidsinstellingen, die gezondheidsinformatie over de gebruiker kunnen prijsgeven. Mogelijk moet de verwerking van die gegevens op grond van het verwerkingsverbod van telemetrie worden uitgesloten.

4.9. Dit verweer slaagt. De essentiële functie van zoekmachines in de huidige, wereldwijd door het internet verbonden, samenlevingen, zou immers onaanvaardbaar worden beperkt als het voor exploitanten van zoekmachines categorisch zou zijn verboden aan het publiek koppelingen ter beschikking te stellen naar publicaties waarin wordt bericht over strafrechtelijke verdenkingen tegen, of strafrechtelijke veroordelingen van medeburgers."

13. Doelbinding

Uit de beschikbare informatie blijkt niet dat Microsoft telemetriegegevens verwerkt of zou willen gaan verwerken voor andere doeleinden (zoals die uiteen zijn gezet in de paragrafen 4 en 6) dan waarvoor het ze zegt te verzamelen. De doelen zijn ook uitdrukkelijk en welbepaald.

Eventueel verder gebruik van telemetriegegevens door de werkgever dient wel getoetst te worden aan de eis van verenigbaarheid. Daarbij is van belang dat diezelfde werkgever als mede-verwerkingsverantwoordelijke bepaalt in welke mate er telemetriegegevens aan Microsoft verzonden worden. Als de werkgever daarvoor een rechtsgrond heeft (dat wil zeggen, het gekozen niveau van telemetrie kan verantwoorden), dan is het daadwerkelijke gebruik van die gegevens voor de betreffende doeleinden als verenigbaar te beoordelen.

14. Noodzaak en evenredigheid

Op deze aspecten zijn wij, voor zover mogelijk, ingegaan onder het kopje "Rechtsgrond" in paragraaf 11.

15. Rechten van de betrokkene

Uit de beschikbare informatie blijkt niet dat Microsoft het voor betrokkenen moeilijk of onmogelijk zou maken om hun rechten, bijvoorbeeld op inzage of verwijdering van hun gegevens, uit te oefenen. Ook de AP heeft in haar onderzoek geen opmerkingen hierover.[49] Overigens biedt de functie "Delete by Device ID"[50] de gebruiker in principe een eenvoudige mogelijkheid om zijn recht op gegevenswissing uit te oefenen; deze functie zal in de praktijk voor werknemers echter niet beschikbaar worden gesteld.[51]

C. Beschrijving en beoordeling risico's voor de betrokkenen

16. Risico's

In deze paragraaf beschrijven en beoordelen we de risico's van telemetrie voor de betrokkenen. Dat zijn vooral de werknemers van overheidsinstanties die met Windows 10 Enterprise werken.

16.1 Analyse

De toelichting in het Model gegevensbeschermingseffectbeoordeling Rijksdienst beveelt de volgende drie stappen aan als het gaat om het in kaart brengen van de risico's:

1. risico's identificeren;
2. risico's inschatten/analyseren;
3. risico's beoordelen/evalueren.

---

[49] Wel merkt de AP op blz. 132 van haar rapport op dat een gebruiker zelfs via de meest uitgebreide informatie die Microsoft ter beschikking stelt geen inzage krijgen in de gegevens die via volledige telemetrie worden verzameld. Het gaat daar echter over de informatieplicht, niet over het recht op inzage.

[50] Zie paragraaf 8 onder het kopje "Verbeteringen voorjaar 2018".

[51] Zie paragraaf 3.

Hieronder lopen we deze aspecten langs voor de mogelijke risico's die het Model benoemt. We gaan daarbij uit van telemetrie op het aanbevolen niveau Security. Het streven is daarbij uiteraard om realistische scenario's in kaart te brengen. Om die reden is onder meer het risico van een bewuste onrechtmatige daad door Microsoft, zoals het verwerken van gegevens op een wijze waarvan het evident is dat die contractueel is uitgesloten, niet in de afwegingen meegenomen.

- *waar de gegevensverwerking kan leiden tot:*
  – discriminatie, stigmatisering en uitsluiting;
  – (blootstelling aan) identiteitsdiefstal of fraude;
  – financiële verliezen;
  – reputatie of anderszins relationele schade;
  – verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens;
  – ongeoorloofde ongedaan making van pseudonimisering;
  – of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie;

Voor de genoemde gevolgen geldt dat er geen aanleiding is om aan te nemen dat Microsoft die met telemetrie op wat voor wijze dan ook beoogt. Dit met onderstaande vier kanttekeningen. De risico's zijn alleen in de context van deze PIA beoordeeld en gewogen.

1) Niet duidelijk is of Microsoft telemetrie binnen Windows 10 Enterprise ook gebruikt voor het doen van gepersonaliseerde aanbiedingen en suggesties. Mocht dat wel het geval zijn, en mochten die gebaseerd zijn op bepaald surfgedrag of het gebruik van bepaalde apps, dan kan dit privé-informatie prijsgeven als anderen meekijken. Zeker bij privégebruik van zakelijke apparaten is dit denkbaar.

Als telemetrie hier al voor wordt ingezet, dan lijkt het onwaarschijnlijk dat dat op zo'n manier zal gebeuren dat daarmee gevoelige gegevens aan de oppervlakte komen. Scenario's waarbij de betrokkene daarvan bovendien daadwerkelijk schade of nadeel ondervindt, lijken niet erg waarschijnlijk.

Conclusie: risico laag

2) Naarmate Microsoft meer telemetriegegevens verzamelt, wordt wel het risico groter dat de gegevens in het geval van een datalek op bovenstaande wijze misbruikt kunnen worden. Denk bijvoorbeeld aan het hierboven genoemde voorbeeld van informatie over surfgedrag of gebruik van apps dat mensen chantabel kan maken.

Dit is een algemeen punt. Naarmate er meer en gevoeligere gegevens bij elkaar worden gebracht, kunnen de gevolgen van een datalek ernstiger zijn. Microsoft heeft er echter zelf ook veel belang bij dat hier niets misgaat: een serieus datalek van telemetriegegevens zou het bedrijf ernstige reputatieschade opleveren.

Conclusie: Risico laag

3) Microsoft combineert bij telemetrie allerlei identifiers, soms direct van personen, veelal indirect van apparaten, die echter doorgaans vrij duidelijk aan een specifieke persoon gelinkt zijn. Mochten telemetriegegevens ook gepseudonimiseerde gegevens bevatten, dan ontstaat er dus een risico op (de mogelijkheid tot) het ongedaan maken van die pseudonimisering.
Voor zover wij dat kunnen overzien, zullen er niet of nauwelijks gepseudonimiseerde gegevens onderdeel uitmaken van de telemetriegegevens. Het risico van ongeoorloofde ongedaanmaking van pseudonimisering zal zich dan niet manifesteren. Een gerelateerd risico dat zich juist wel zal manifesteren is het koppelen aan personen en aan elkaar van verschillende (apparaat)identifiers (en daarmee van de achterliggende gegevens). Die koppeling kan ook buiten de context van

telemetrie zeer interessant zijn: zij zou Microsoft bijvoorbeeld in staat kunnen stellen om telemetriegegevens te combineren met LinkedIn-profielen. Er zijn overigens geen aanwijzingen dat Microsoft de gegevens op deze wijze verder zou willen gebruiken.

Conclusie: Risico laag

4) Een niet expliciet benoemd risico voor de betrokkene is een mogelijk nadelige impact op zijn veiligheid. Zo zal het in het algemeen mogelijk zijn om uit locatiegegevens af te leiden bij welke overheidsinstantie iemand werkzaam is. Dit kan een veiligheidsrisico opleveren, met name voor werknemers in gevoelige of geheime posities. Daar staat tegenover dat telemetrie op niveau Security juist ook helpt om het apparaat te beveiligen tegen hacken, waarbij nog veel meer en gevoeligere gegevens over de werknemer buit zouden kunnen worden gemaakt. Naar onze inschatting zullen de veiligheidsvoordelen van telemetrie op niveau Security in het algemeen zwaarder wegen dan de veiligheidsrisico's. Individuele overheidsinstanties kunnen uiteraard op grond van specifieke voor hen geldende omstandigheden tot een andere afweging komen.

Conclusie: Informatie veiligheidsrisico hoog, risico in het kader van persoonsgegevensverwerkingen laag

- *wanneer de betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd om controle over hun persoonsgegevens uit te oefenen;*

Dit is een reëel risico. De opdrachtgever heeft aangegeven dat het vanuit beheersperspectief in het algemeen onwenselijk is om werknemers individuele keuzes te geven als het gaat om telemetrie. De werknemer is daarmee feitelijk "veroordeeld" tot de keuzes die de werkgever voor hem maakt. Daarmee heeft de medewerker geen (althans beperkte) controle over zijn persoonsgegevens. Indien telemetrie ook wordt gebruikt voor het doen van gerichte aanbiedingen, dan is in het bijzonder het absolute recht van verzet tegen het gebruik van gegevens voor direct marketing in het geding.

Dat een werknemer binnen het kader van de arbeidsrelatie bepaalde rechten en vrijheden niet of in mindere mate kan uitoefenen, en een zekere mate van controle over zijn persoonsgegevens ontbeert, is in zekere zin echter "part of the deal". Wat op dit vlak wel en niet acceptabel is, wordt in abstracte zin bepaald door de eisen van goed werkgeverschap en goed werknemerschap. De werknemer zal inbreuken tot op zekere hoogte moeten tolereren, de werkgever dient ze tot een aanvaardbaar niveau te beperken. Aangezien er een duidelijke grondslag lijkt te zijn voor het toepassen van een zekere mate van telemetrie, zal de werknemer dit in beginsel moeten accepteren. Dat moet er echter niet toe leiden dat hem zijn fundamentele rechten onder de AVG ontnomen worden, of het nu gaat om zijn relatie met Microsoft of om die met zijn werkgever.[52]

Conclusie: Risico hoog

- *wanneer bijzondere of strafrechtelijke persoonsgegevens worden verwerkt;*

Dit is in feite een verzwarende omstandigheid. Het verwerken van zulke gegevens op zich is geen specifiek risico. De hierboven genoemde risico's kunnen echter grotere impact hebben als ze zich voordoen in de context van bijzondere gegevens.

[52] Volgens de richtsnoeren van de artikel 29 Werkgroep is in dit soort situaties in principe een DPIA aangewezen. Aangezien hier sprake is van een zgn. 'captive relationship' is een DPIA echter niet nodig.

Bij telemetrie op niveau Security worden er niet gericht bijzondere gegevens verzameld.[53] Deze verzwarende omstandigheid kan zich in de praktijk niettemin voordoen, aangezien bijv. crash dumps delen van de inhoud van bestanden kunnen bevatten. Zulke gegevens worden op niveau Security echter slechts beperkt verwerkt; de kans dat er herleidbare bijzondere gegevens tussen zitten, en dat die dan ook nog eens gericht misbruikt of oneigenlijk gebruikt worden door Microsoft, schatten wij in als zeer laag.

Conclusie: Risico laag

- *wanneer persoonlijke aspecten worden geëvalueerd, om bijvoorbeeld beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken;*

Dit is een indirect risico. Wat is het feitelijke nadeel of de feitelijke schade die de medewerker kan ondervinden van de profilering? Met uitzondering van het personaliseren van interfaces en targeting voor reclamedoeleinden[54] is telemetrie niet gericht op consequenties voor de individuele gebruiker.

Conclusie: Risico Laag

- *wanneer persoonsgegevens van kwetsbare personen, zoals kinderen, worden verwerkt;*

Dit risico doet zich voor, aangezien de werknemer in zekere mate afhankelijk is van de werkgever. Op dit aspect zijn we al ingegaan onder de bullet "*wanneer bijzondere of strafrechtelijke persoonsgegevens worden verwerkt* hierboven.

- *wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen.*

Het gaat zonder twijfel om het verwerken van een grote hoeveelheid gegevens over een groot aantal betrokkenen. De verwerking heeft echter slechts in beperkte mate ook gevolgen voor die betrokkenen.

Conclusie: Risico Laag

Het bovenstaande overziende schatten wij de privacyrisico's van telemetrie op niveau Security in als laag

16.2 Conclusies

Op basis van de analyse in de vorige deelparagraaf trekken wij de volgende conclusies.

[53] Voor niveau Basic gaat die bewerking mogelijk niet helemaal op. Wij denken met name aan toegankelijkheidsinstellingen. Die geven in veel gevallen vrij specifieke informatie prijs over de gezondheidstoestand van de betrokkene, en zijn dus aan te merken als bijzondere gegevens. Niet duidelijk is in hoeverre zulke gegevens worden verzameld bij telemetrie op niveau Basic. Voor zover dat wel het geval is, valt de verwerking van die gegevens overigens waarschijnlijk niet onder het verwerkingsverbod van bijzondere gegevens, aangezien een beroep kan worden gedaan op de uitzondering in art. 9 lid 2 onder b AVG.
[54] Indien dat laatste onderdeel uitmaakt van telemetrie in Windows 10 Enterprise.

Telemetrie brengt risico's met zich mee voor de persoonlijke levenssfeer en de rechten en vrijheden van de betrokken werknemers.

Die risico's zijn echter beperkt in omvang. Deze conclusie is echter alleen gewettigd omdat telemetrie (vrijwel) geen effecten beoogt voor de individuele eindgebruiker, en Microsoft (naar eigen zeggen) AVG-compliant werkt.

De mogelijke risico's kunnen verder beperkt worden door te kiezen voor telemetrieniveau Security. De nadelige gevolgen daarvan qua functionaliteit zijn beperkt.

Bij deze conclusies zijn de onderstaande twee kanttekeningen te plaatsen.

- Het is moeilijk om zicht te krijgen op wat Microsoft precies doet, en er zijn geen zekerheden dat de werkwijze van Microsoft in de toekomst niet gaat veranderen. De vraag kan dan ook opgeworpen worden of een risico dat momenteel niet bestaat (althans niet lijkt te bestaan) zich niet in de toekomst alsnog zal manifesteren, met name doordat Microsoft wijzigingen aanbrengt in het doel of de middelen (= de wijze van verwerken) van telemetrie. Aangezien de meeste telemetriegegevens voor een relatief beperkte tijd worden bewaard (30 dagen) zijn de directe risico's hiervan voor de betrokkenen beperkt, ervan uitgaande dat de overheidsinstantie zich zal beraden op hoe zij omgaat met telemetrie mocht deze situatie zich voordoen. Het risico blijft er dan toe beperkt dat de telemetriegegevens die op dat moment bij Microsoft berusten voor nieuwe doeleinden of op andere wijze verwerkt worden. Wij zien echter niet in dat Microsoft, alles afwegende, een reëel belang heeft bij dat laatste scenario. We beperken ons daarom bij de risico-inventarisatie tot de huidige wijze van verwerken van telemetriegegevens. Dat neemt niet weg dat hier wel sprake is van een organisatierisico: het heroverwegen van de positie m.b.t. telemetrie kan grote consequenties hebben, bijvoorbeeld als de conclusie zou moeten zijn dat het gebruik van de software niet langer rechtmatig is. Het is immers de vraag hoe reëel het is om in plaats van Windows 10 een ander bedrijfssysteem te gaan gebruiken. Misschien echter nog wel belangrijker dan het risico van 'schuivende panelen' (function creep) aan de zijde van Microsoft is juist de hier benoemde onduidelijkheid zelf. Het geheel aan voorwaarden van, en afspraken en overeenkomsten met Microsoft is een zo complex geheel dat dit zelfs voor specialisten niet of nauwelijks te doorgronden is. Een reëel en aanzienlijk risico is daarmee dat aan beide zijden, maar toch vooral bij de klant, onduidelijk is wat nu feitelijk de afspraken zijn.
- De focus in onze analyse ligt op de gegevens van de werknemer. Er is daarnaast een mogelijkheid dat er bij telemetrie gegevens worden verwerkt van burgers of andere betrokkenen. Het gaat dan om bijv. crash dumps die delen van gebruikersbestanden kunnen bevatten. Het valt niet helemaal uit te sluiten dat van zulke gegevens misbruik kan worden gemaakt dat ernstige gevolgen heeft voor de betrokkene. De kans dat dergelijke gegevens in het kader van telemetrie naar Microsoft gaan, schatten wij bij een keuze voor niveau Security echter zeer laag in. Hetzelfde geldt voor het risico dat er in zulke situaties, mochten ze zich niettemin voordoen, ook daadwerkelijk misbruik zal worden gemaakt van de gegevens.

Tot slot het volgende. In deze DPIA ligt de nadruk op de risico's voor betrokkenen. Die vertalen zich echter veelal in risico's voor de organisatie. Zoals we in de inleiding van dit rapport al hebben aangegeven, zal er behalve naar de privacyrisico's ook naar de veiligheidsrisico's gekeken moeten worden. In dat licht merken wij op dat wij het bij de huidige inrichting en doeleinden van telemetrie onwaarschijnlijk achten dat een vorm en mate van telemetrie die aanvaardbaar zijn vanuit het

oogpunt van onder meer informatiebeveiliging en staatsveiligheid, niet aanvaardbaar zouden zijn vanuit het oogpunt van privacy.

D. Beschrijving voorgenomen maatregelen

17. Maatregelen

Een typische DPIA wordt uitgevoerd door (of in opdracht van) de verwerkingsverantwoordelijke. De vraag die die in dat geval hier primair dient te beantwoorden, is welke beheersmaatregelen hij in redelijkheid kan treffen (of eventueel door verwerkers kan laten treffen) om de geconstateerde risico's tot een aanvaardbaar niveau terug te brengen.

Deze DPIA voeren wij echter niet uit in opdracht van de verwerkingsverantwoordelijken, maar in opdracht van de inkooporganisatie. Daarmee moet de bredere vraag beantwoord worden welke beheersmaatregelen zowel de inkooporganisatie als de verwerkingsverantwoordelijken zouden kunnen of moeten treffen. Ook hier geldt dat het vooral aan Microsoft zelf is om als belangrijkste verantwoordelijke voor telemetrie de benodigde beheersmaatregelen te treffen; voor zover mogelijk hebben we deze maatregelen in dit rapport marginaal beoordeeld. Tegelijkertijd noopt de beperkte mede-verantwoordelijkheid van de overheidsinstantie die gebruik maakt van de software, maar meer nog de eis van goed werkgeverschap, tot het treffen van beheersmaatregelen. De belangrijkste daarvan zetten we hieronder op een rijtje. De overheidsinstantie zal altijd moeten beoordelen of in haar specifieke context aanvullende maatregelen nodig zijn. Tot slot kunnen een aantal zaken beter op het niveau van de inkooporganisatie worden opgepakt. Ook daarvan zetten we de belangrijkste op een rij.

17.1 Overheidsinstantie

De overheidsinstantie is medeverantwoordelijke omdat zij bepaalt in welke mate Microsoft wordt toegestaan om telemetriegegevens te verzamelen (zie paragraaf 5). Bovendien dient zij invulling te geven aan de eis van goed werkgeverschap.

De belangrijkste beheersmaatregel die zij kan treffen is dan ook het weloverwogen kiezen voor een bepaald niveau van telemetrie. In paragraaf 11.2 hebben wij onderbouwd de aanbeveling gedaan om te kiezen voor het niveau Security.

Om Windows 10 te kunnen gebruiken moet een gebruiker een account aanmaken. Dit kan een Microsoft-account zijn, of een lokaal account, dat alleen op het betreffende apparaat bestaat. Het gebruik van lokale accounts verkleint de mogelijkheden van Microsoft om gegevens aan elkaar te

koppelen. Een aanbeveling is dan ook om indien dat mogelijk is gebruikers te verplichten, of althans de mogelijkheid te bieden, om Windows 10 met een lokaal account te gebruiken.

De door de overheidsinstantie te nemen beheersmaatregelen zijn de volgende.

- Kies voor telemetrieniveau Security.

- Laat medewerkers zoveel mogelijk van Windows gebruik maken met een lokaal account.

- Voer als daar aanleiding voor is een aanvullende privacyrisicoanalyse uit.

Een beheersmaatregel die verder voor de hand ligt is het maken en schriftelijk vastleggen van afspraken met Microsoft over de onderlinge verdeling van verantwoordelijkheden. Dit is immers verplicht op basis van art. 26 AVG. In de praktijk zullen deze afspraken echter, uitzonderingen daargelaten, niet gemaakt worden door individuele overheidsinstanties, maar centraal door SLM Microsoft Rijk. We behandelen deze maatregel daarom in de volgende paragraaf. Hetzelfde geldt voor het monitoren van het feitelijke telemetrieverkeer.

17.2 SLM Microsoft Rijk

De meest evidente door SLM Microsoft Rijk te nemen beheersmaatregel is het namens de afnemende overheidsinstanties maken van de hierboven genoemde, op grond van art. 26 AVG verplichte, afspraken over het verdelen van de gezamenlijke verantwoordelijkheid. In deze afspraken moeten zaken worden geregeld zoals het afhandelen van verzoeken van betrokkenen en het melden van datalekken. Een complicatie hierbij kan zijn dat Microsoft niet genegen is om zijn medewerking te verlenen aan het maken van zulke afspraken. Het stelt zich immers op het standpunt, dat het als enige verwerkingsverantwoordelijke is voor telemetrie.[55] Het risico voor de overheid lijkt ons in dat geval beperkt. Wanneer zij er van haar kant alles aan doet om tot de verplichte afspraken te komen, maar Microsoft dat weigert, dan zal bijvoorbeeld de AP in een onderzoek waarschijnlijk Microsoft ook verantwoordelijk houden voor non-compliance op dit vlak. Niet uit te sluiten is natuurlijk dat de AP een ander standpunt inneemt over het vraagstuk van de verantwoordelijkheidsverdeling. Te overwegen valt daarom om de AP op dit specifieke punt om een formele zienswijze te vragen.

Meer winst valt er te behalen bij de overige (bestaande) overeenkomsten met Microsoft. In ieder geval kan SLM Microsoft Rijk er naar streven dat er volstrekt duidelijke en eenduidige terminologie gehanteerd wordt. Meer in het algemeen is het geheel aan voorwaarden van, en afspraken en overeenkomsten met Microsoft een zo complex geheel dat dit zelfs voor specialisten niet of nauwelijks te doorgronden is. Het verdient daarom nadrukkelijk aanbeveling om daarover via contractuele afspraken duidelijkheid c.q. garanties van Microsoft te verkrijgen. Het gaat dan dus niet om nieuwe of aanvullende afspraken of garanties, maar om het in klare taal formuleren en door Microsoft laten bevestigen van wat de essentie is van de gemaakte afspraken over voor de Nederlandse overheid wezenlijke zaken. Welke zaken dat precies zijn zal nader in kaart gebracht moeten worden. Op basis van de inhoud van deze DPIA kunnen wij in ieder geval de volgende in onze optiek essentiële zaken benoemen:

- Het hanteren van duidelijke en eenduidige definities.
- Het nader uitwerken en specificeren van de doeleinden waarvoor Microsoft telemetrie toepast.
- Het scheppen van duidelijkheid over welke onderdelen van het Microsoftconcern welke telemetriegegevens verwerken.

[55] Zie bijlage 1, paragraaf 4.

- Microsoft en de overheidsinstantie zijn gezamenlijke verwerkingsverantwoordelijken voor de overdracht van telemetriegegevens naar Microsoft.
- Microsoft erkent dat telemetriegegevens persoonsgegevens zijn.
- Microsoft houdt zijn DPIA op Windows 10 actueel en beschikbaar.
- Microsoft koppelt gegevens waarover het als verwerker beschikt niet met gegevens waarover het als verwerkingsverantwoordelijke beschikt.
- Microsoft gebruikt Windows 10 Enterprise telemetriegegevens niet voor direct marketing. In het bijzonder verwerkt het geen Reclame ID van gebruikers van Windows 10 Enterprise.
- Microsoft verwerkt in Windows 10 Enterprise geen telemetriegegevens met als rechtsgrond de toestemming van de werknemer.

Uiteraard kan het ook zo zijn dat SLM Microsoft Rijk bepaalde hier geconstateerde risico's zo hoog inschat dat het daarover wel aanvullende afspraken met Microsoft wil (proberen te) maken.

Verder kan SLM Microsoft Rijk namens de overheidsinstanties als mede-verwerkingsverantwoordelijken op technisch niveau monitoren welke gegevensoverdracht er in het kader van telemetrie feitelijk plaatsvindt.

De door SLM Microsoft Rijk te nemen beheersmaatregelen zijn de volgende.

- Sluit namens de individuele overheidorganisaties een art. 26-overeenkomst met Microsoft.

- Laat Microsoft een verduidelijkend document tekenen waarin in ieder geval de in paragraaf 17.2 benoemde essentiële zaken in klare taal staan beschreven.

- Maak, als je bepaalde risico's als te hoog inschat, aanvullende afspraken met Microsoft.

- Monitor welke gegevensoverdracht er in het kader van telemetrie feitelijk plaatsvindt.

17.3 Restrisico's

Wanneer overheidsinstanties en SLM Microsoft Rijk de hierboven aanbevolen maatregelen nemen, is er binnen de beoordelingscontext van deze DPIA sprake van alleszins acceptabele restrisico's voor de bescherming van de persoonsgegevens van de betrokken werknemers. Ernstigere restrisico's kunnen echter juist in die beoordelingscontext besloten liggen. Zoals we bij herhaling hebben aangegeven, blijkt het zeer lastig om op basis van de beschikbare documentatie en informatie een afgerond beeld te krijgen van telemetrie. Een meer dan marginale inhoudelijke beoordeling van de verwerking van telemetriegegevens door Microsoft is mede daarom praktisch gezien niet mogelijk. En het is zeer de vraag of dat binnen afzienbare tijd gaat veranderen.

Dat hoeft echter geen probleem te zijn. Zoals we hebben uiteengezet in paragraaf 11 is het primair aan Microsoft om haar verwerking van telemetriegegevens AVG-compliant in te richten. Het is aan DI&I om zich namens de Nederlandse overheid op hoofdlijnen een beeld te vormen van de aard, juistheid en effectiviteit van de maatregelen die Microsoft op dat vlak neemt. We doelen dan dus niet zozeer op de concrete details van de inrichting van de verwerking, maar meer op alle organisatorische maatregelen daaromheen. Ofwel: op privacymanagement conform het verantwoordingsbeginsel ("accountability'") van art. 24 lid 1 AVG. Hoewel er zeker wel het een en ander valt op te merken over de inspanningen van Microsoft op dit vlak (denk aan gebrek aan transparantie, complexiteit, onduidelijkheid over gehanteerde termen en nagestreefde doeleinden, relatie van die laatste met de feitelijk verwerkte gegevens), is onze indruk dat Microsoft er in essentie naar streeft om zowel naar de letter als naar de geest de AVG na te leven. Wanneer DI&I deze zienswijze deelt, dan ligt als beheersmaatregel voor de hand dat zij over

gegevensbescherming een constructief kritische dialoog met Microsoft entameert, die erop gericht is dat Microsoft zich structureel en effectief gaat verantwoorden over haar verwerking van telemetriegegevens. Zo lang een dergelijke dialoog mogelijk is en productief blijkt, is naar onze inschatting ook het hier besproken "meta-restrisico" acceptabel.

Met deze laatste constatering is nog geen antwoord gegeven op de vraag welke beheersmaatregelen er op dit moment in ieder geval moeten worden genomen zijn om te kunnen spreken van aanvaardbare restrisico's. Naar ons oordeel zijn dit de onderstaande.

De minimaal te nemen beheersmaatregelen om op dit moment te kunnen spreken van aanvaardbare restrisico's zijn de volgende.

Overheidsinstantie

- Kies voor telemetrieniveau Security.

- Voer als daar aanleiding voor is een aanvullende privacyrisicoanalyse uit.

SLM Microsoft Rijk (DI&I)

- Sluit namens de individuele overheidorganisaties een art. 26-overeenkomst met Microsoft.

- Laat Microsoft een verduidelijkend document tekenen waarin in ieder geval de in paragraaf 17.2 benoemde essentiële zaken in klare taal staan beschreven.

Bijlage 1 – Rollen onder de AVG bij het verwerken van telemetriegegevens

1. Inleiding

In deze bijlage worden, aan de hand van de onderlinge afspraken, de rollen en bevoegdheden onder de AVG uitgewerkt van de diverse partijen die betrokken zijn bij het verwerken van telemetriegegevens.[56]

Deze partijen zijn:

- Het Ministerie van Justitie en Veiligheid, Directie Infomatievoorziening en Inkoop ("DI&I");
- De overheidsinstanties die gebruik maken van Windows 10 Enterprise ("de werkgevers");
- Microsoft Corporation ("Microsoft").

De onderlinge relaties tussen de genoemde partijen worden beheerst door een aantal documenten, zie hiervoor paragraaf 9.

2. Rollen onder de AVG

Om de rol van de betrokken partijen te kunnen duiden is het van belang om de relevante wettelijke begrippen nader te benoemen. De AVG kent twee fundamentele rollen als het gaat om het verwerken van persoonsgegevens, te weten:

- de verwerkingsverantwoordelijke[57]
- de verwerker[58]

Het begrip 'verwerkingsverantwoordelijke' speelt in de AVG een centrale rol. Op de verwerkingsverantwoordelijke rust namelijk de plicht om de kernverplichtingen van de AVG na te leven.[59] Ook is de verwerkingsverantwoordelijke (hoofdelijk) aansprakelijk voor de schade of het nadeel dat voortvloeit uit het niet-nakomen van de voorschriften van de AVG.[60] Complexe gegevensstromen en afspraken tussen meerdere partijen maken het vaak lastig om vast te stellen wie in een specifiek geval de verwerkingsverantwoordelijke is. Het is voor een bij de verwerking betrokken organisatie niet mogelijk om *geen* verantwoordelijke of verwerker te zijn. Wanneer een partij zelf persoonsgegevens verwerkt, dan is die ofwel verantwoordelijke, ofwel verwerker; andere mogelijkheden zijn er juridisch gezien niet. Een partij die niet zelf persoonsgegevens verwerkt, kan overigens ook (mede)verantwoordelijke zijn, en wel als die invloed uitoefent op de verwerking (zie paragraaf 5). Omdat er bij telemetrie sprake is van meerdere betrokken partijen, en complexe gegevensstromen en afspraken, is het van belang om precies vast te stellen wie welke rol heeft met betrekking tot de verwerking van telemetriegegevens.

3. Het begrip 'verwerkingsverantwoordelijke'

Artikel 4(7) AVG definieert de verwerkingsverantwoordelijke als: *een natuurlijke persoon of*

---

[56] De verwerkersovereenkomsten tussen de verschillende actoren laten we bij deze analyse buiten beschouwing. Deze volgen immers primair het antwoord op de vraag wie verwerkingsverantwoordelijke of verwerker is. Deze rollen worden niet gevestigd uitsluitend door het sluiten van een verwerkersovereenkomst.

[57] Art. 4(7) AVG.

[58] Art. 4(8) AVG.

[59] Art. 5(2) AVG.

[60] Art. 82(2) AVG.

rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

De Artikel 29 Werkgroep heeft over het begrip 'verwerkingsverantwoordelijke' een advies uitgebracht.[61] In dit advies wordt gesteld dat het begrip 'verwerkingsverantwoordelijke' zowel een autonoom als een functioneel begrip is. Met 'autonoom' wordt bedoeld dat het met name dient te worden geïnterpreteerd volgens de communautaire wetgeving voor gegevensbescherming.[62] Met 'functioneel' wordt bedoeld dat het begrip 'verwerkingsverantwoordelijke' bedoeld is om de verantwoordelijkheden te leggen op de plaats waar ook de feitelijke invloed ligt, en dus eerder op een feitelijke dan op een formele analyse moet worden gebaseerd.

De definitie in de richtlijn is opgebouwd uit drie hoofdonderdelen:
- het personele aspect ("*een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan*"),
- de mogelijkheid van gezamenlijke verantwoordelijkheid ("*die/dat, alleen of samen met anderen,*"),
- de wezenlijke aspecten waarmee de verwerkingsverantwoordelijke van andere partijen kan worden onderscheiden ("*het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt*").

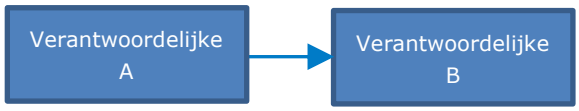
Hieronder zullen we kortheidshalve in plaats van de 'verwerkingsverantwoordelijke' spreken van de 'verantwoordelijke'.

3.1. Medeverantwoordelijkheid

De AVG laat de mogelijkheid toe dat er niet één, maar twee of meer verantwoordelijken zijn voor een verwerking. Indien er sprake is van meerdere verantwoordelijken voor één verwerking, dan worden zij 'gezamenlijke verantwoordelijken' genoemd.[63]

Er zijn vier basistypen samenwerkingen tussen twee of meer verantwoordelijken te onderscheiden. Hieronder worden deze samenwerkingsvormen nader toegelicht.

(i) Alle actoren zijn zelfstandig verantwoordelijk



Verantwoordelijke A verstrekt eenmalig of structureel persoonsgegevens aan B, zodat B deze verder kan gebruiken. Zowel A als B verwerken de persoonsgegevens vanwege hun eigen doeleinden en op grond van hun eigen rechtsgronden onder artikel 5(1) AVG. In dit model is er *geen* sprake van medeverantwoordelijkheid. De verantwoordelijkheid (en de aansprakelijkheid) is voor iedere verantwoordelijke beperkt tot de eigen verwerking. In dit model is A dus verantwoordelijk voor de verstrekking aan B, hoewel het niet uitgesloten is dat B verantwoordelijke is voor de beveiliging van het communicatiekanaal indien dat door A op aanwijzing van B gebruikt wordt. Denk bij dit model bijvoorbeeld aan een werkgever (verantwoordelijke A) die loonbelastinggegevens moet verstrekken aan de Belastingdienst

[61] Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", 16 februari 2010, 00264/10/NL, WP169.
[62] Ten tijde van het advies met name Richtlijn 95/46/EG, tegenwoordig met name de AVG.
[63] Hoewel wij de uitspraak "gezamenlijke verantwoordelijkheid is geen verantwoordelijkheid" begrijpen vanuit het oogpunt van het (al dan niet) *nemen* van verantwoordelijkheid, is het juridisch gezien onjuist om de mogelijkheid van het bestaan van gezamenlijke verwerkingsverantwoordelijkheid af te wijzen.

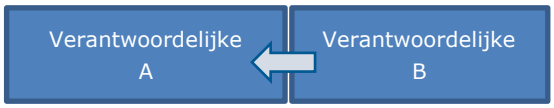
(verantwoordelijke B), of aan TransLink (verantwoordelijke A) dat met het oog op fraudebestrijding op vrijwillige basis reisgegevens van studenten verstrekt aan DUO (verantwoordelijke B).

In het voorgaande scenario is er zoals gezegd geen sprake van 'medeverantwoordelijkheid'. Dit is wel het geval bij de onderstaande scenario's (ii) t/m (iv).

(ii) Afzonderlijke verantwoordelijkheid

In dit model is er sprake van een min of meer geïntegreerde verwerking van persoonsgegevens door meerdere verantwoordelijken, waarbij echter iedere verantwoordelijke het gezamenlijke systeem afzonderlijk (lees: ieder voor *eigen* doeleinden) gebruikt. Dit model is bijvoorbeeld van toepassing op het in de lucht hebben van één technisch systeem (platform, infrastructuur) dat door beide verantwoordelijken A en B ieder voor zich wordt gebruikt. Denk bijvoorbeeld aan technisch één salarisadministratiesysteem dat door de afzonderlijke groepsmaatschappijen binnen een concern wordt gebruikt. In dit geval zijn de verantwoordelijkheden (en de aansprakelijkheden) van A en B beperkt tot hun eigen verwerking met behulp van het systeem. In de praktijk zal daarnaast een van beide verantwoordelijken (namelijk die, die het systeem beheert) ook verwerker zijn voor de andere verantwoordelijke.

(iii) Gemeenschappelijke verantwoordelijkheid



Dit is een variant van scenario (ii), waarbij verantwoordelijke B de verantwoordelijkheid (en de aansprakelijkheid) geheel of gedeeltelijk heeft overgedragen aan verantwoordelijke A. Dit model komt vaak voor in concerns, waar het hoofdkantoor of een *shared service center* (A) een gemeenschappelijke verwerking in de lucht brengt voor de aangesloten groepsmaatschappijen (B), die meestal verplicht zijn om dit systeem te gebruiken bij de uitvoering van hun eigen bedrijfsprocessen.

In dit scenario kunnen twee sub-varianten worden onderscheiden:
- *Volledige gemeenschappelijke verantwoordelijkheid*: Als de verantwoordelijkheid *geheel* is overgedragen, is A *als enige* verantwoordelijke (en aansprakelijk) voor de gemeenschappelijke verwerking; B is geen verantwoordelijke meer en ook niet meer aansprakelijk. B is echter wel gebruiker van het systeem. De non-compliance van B wordt toegerekend aan A. Er is na de overdracht van de verantwoordelijkheid dus geen sprake meer van 'medeverantwoordelijkheid' van B; A is de enige verantwoordelijke.

- *Onvolledige gemeenschappelijke verantwoordelijkheid*: Maar vaker komt het voor dat alleen de *systeemverantwoordelijkheid* in meerdere of mindere mate aan A is overgedragen. A stelt dan als enige het *algemene* doel van het systeem vast (waaronder het besluit tot het in de lucht brengen van het systeem), en ook de *gemeenschappelijke* middelen, zoals het technische systeem en de structurele gegevensstromen, de beveiligingsmaatregelen en het eventuele uitbesteden van de verwerking aan een verwerker. Voor al deze zaken is A als enige de verantwoordelijke (en ook als enige aansprakelijk). De rol van de B is gereduceerd tot die van

gebruiksverantwoordelijke. B blijft verantwoordelijke (en aansprakelijk) voor zijn eigen gebruik van het systeem en het gebruik ervan voor zijn eigen bedrijfsprocessen, zoals het vastleggen en het raadplegen van de persoonsgegevens, het verstrekken van de persoonsgegevens aan derden, en bepalen wie binnen de organisatie van B toegang heeft tot de persoonsgegevens.

(iv) Hoofdelijke verantwoordelijkheid

In dit scenario is er sprake van verschillende verwerkingen die zijn geïntegreerd tot één gezamenlijke verwerking zonder dat er een gemeenschappelijke verantwoordelijke (iii) als in scenario aanwezig is. Er is sprake van volledige gezamenlijke verantwoordelijkheid en elk van de verantwoordelijken is hoofdelijk aansprakelijk voor het geheel van de gegevensverwerkingen. Te denken valt aan een verwerking waarmee A en B een gemeenschappelijk doel nastreven, zoals een gemeenschappelijke zwarte lijst. Maar ook bij scenario's (ii) en (iii, onvolledige verantwoordelijkheid) kan er sprake zijn van hoofdelijke verantwoordelijkheid. Dat is het geval als er onvoldoende afspraken zijn gemaakt tussen de verantwoordelijken of deze onvoldoende met de betrokkene zijn gecommuniceerd, dat het onvoldoende duidelijk is hoe de verantwoordelijkheden zijn verdeeld.

3.2. Vaststellen doel en middelen

De verantwoordelijke stelt (alleen of samen met anderen) het doel en de middelen van de verwerking vast. Het is belangrijk om te begrijpen dat een partij verantwoordelijk kan zijn voor de verwerking, ongeacht of zij bij wet is aangewezen als verwerkingsverantwoordelijke. Sterker nog, dat laatste is slechts zelden het geval. De hoedanigheid van verwerkingsverantwoordelijke is doorgaans het gevolg van de feitelijke omstandigheid dat een partij heeft besloten om persoonsgegevens voor eigen doeleinden te verwerken. Een zuiver formeel criterium zou om ten minste twee redenen niet toereikend zijn: in bepaalde gevallen zou een formele aanstelling van een voor de verwerking verantwoordelijke – bijvoorbeeld in een wet, contract of aanmelding bij de autoriteit voor gegevensbescherming – gewoonweg ontbreken. In andere gevallen kan het voorkomen dat de formele aanstelling niet de realiteit weergeeft, bijvoorbeeld wanneer de rol van voor de verwerking verantwoordelijke formeel wordt toegekend aan een instantie die feitelijk niet in een positie verkeert om "vast te stellen".[64] Het is niet relevant of het besluit om gegevens te verwerken "rechtmatig" was in die zin dat de partij die een dergelijk besluit nam daartoe juridisch bevoegd was, noch dat een voor de verwerking verantwoordelijke formeel werd aangesteld volgens een specifieke procedure.[65]

Het begrip "verwerkingsverantwoordelijke" is een functioneel begrip, dat is bedoeld om verantwoordelijkheden te leggen op de plaats waar de feitelijke invloed ligt. Het is dus meer op een feitelijke dan op een formele analyse gebaseerd.[66] De Artikel 29 Werkgroep komt tot onderstaande indeling in drie typen verantwoordelijken, al naar gelang het aangrijpingspunt voor verwerkingsverantwoordelijkheid.

[64] WP169, blz. 10/11.
[65] WP169, blz. 11.
[66] WP169, blz. 12.

- Formele verantwoordelijkheid (expliciete bevoegdheid), d.w.z. de verantwoordelijkheid vloeit voort uit een expliciete wettelijke bevoegdheid. Hiervan is sprake wanneer de verwerkingsverantwoordelijke bij wet wordt aangesteld of de opdracht of plicht tot het verzamelen en verwerken van bepaalde gegevens bij wet is geregeld. Zo is de Minister van Financiën de verwerkingsverantwoordelijke als het gaat om de persoonsgegevens die de Belastingdienst verwerkt over de belastingplichtigen.

- Functionele verantwoordelijkheid (impliciete bevoegdheid), d.w.z. de verantwoordelijkheid vloeit voort uit een impliciete bevoegdheid, zoals gemeenrechtelijke bepalingen of vaste juridische praktijken zoals het handelsrecht of het arbeidsrecht. In dit geval kan mede aan de hand van bestaande traditionele rollen, die doorgaans een bepaalde verantwoordelijkheid inhouden, worden vastgesteld wie voor de verwerking verantwoordelijk is. De bevoegdheid om verwerkingsactiviteiten vast te stellen is uit de aard der zaak gekoppeld aan de functionele rol van een organisatie waaraan uiteindelijk bepaalde verantwoordelijkheden zijn verbonden, ook vanuit een oogpunt van gegevensbescherming.[67] Zo is de werkgever verantwoordelijke voor de persoonsgegevens die hij verwerkt over zijn medewerkers.[68]

- Feitelijke verantwoordelijkheid (invloed), d.w.z. de verantwoordelijkheid wordt in dit geval toegewezen op basis van een beoordeling van de feitelijke omstandigheden. In veel gevallen wordt hiervoor een beoordeling gemaakt van de contractuele verhoudingen tussen de verschillende betrokken partijen. Op grond van deze beoordeling kunnen externe conclusies worden getrokken, waarbij de rol en verantwoordelijkheden van de voor de verwerking verantwoordelijke bij één of meer partijen worden neergelegd. Mogelijk wordt in een contract niets gezegd over de verantwoordelijkheid voor de verwerking, maar bevat het wel voldoende gegevens om de verantwoordelijkheid voor de verwerking te leggen bij een partij die klaarblijkelijk in dit opzicht een leidende rol vervult.[69]
  Het enkele feit dat iemand bepaalt op welke manier persoonsgegevens worden verwerkt, kan ertoe leiden dat hij wordt aangemerkt als voor de verwerking van de gegevens verantwoordelijk, hoewel deze kwalificatie buiten de werkingssfeer van een contractuele verhouding ontstaat of uitdrukkelijk door een contract wordt uitgesloten. Daarnaast kunnen ook andere feiten nuttig zijn om vast te stellen wie voor de verwerking verantwoordelijk is, bijvoorbeeld de mate van feitelijke zeggenschap van een partij.[70] Dit laatste is met name van belang voor verwerkers, die persoonsgegevens verwerken buiten de scope van hun contractuele bevoegdheden. Zij worden voor die beslissingen dan aangemerkt als verantwoordelijke.[71]

4. Rollen bij telemetrie

Het gebruik van telemetrie is een door Microsoft geïnitieerde en uitgevoerde activiteit, die primair ook de doeleinden van Microsoft dient. Microsoft stelt per telemetrieniveau vast welke gegevens het voor welke doeleinden verzamelt. Daarmee stelt Microsoft doel en middelen van de verwerking

---

[67] WP169, blz. 12/13.
[68] NB. Dit betekent *niet* dat de functionele verwerkingsverantwoordelijke (bijv. de werkgever) ook verantwoordelijk is voor de verwerkingen die andere verwerkingsverantwoordelijken uitvoeren met de gegevens die zij van die functionele verantwoordelijke hebben gekregen. Diens verantwoordelijkheid houdt op zodra de gegevens (rechtmatig) zijn overgedragen. Wel kan er onder omstandigheden een situatie van medeverantwoordelijkheid ontstaan (zie paragraaf 5).
[69] WP169, blz. 14.
[70] WP169, blz. 14.
[71] Zie ook het advies van de Artikel 29 Werkgroep inzake Society for Worldwide Interbank Financial Telecommunication (SWIFT), 22 november 2006 (WP 128).

vast, en is het dus verwerkingsverantwoordelijke voor de verzending van telemetriegegevens. Echter, de overheidsinstantie heeft ook een weliswaar beperkte maar niet onbelangrijke invloed op de gegevensverwerking. Zij kan immers voor al haar werknemers instellen welke telemetriegegevens er daadwerkelijk naar Microsoft. Op die keuze heeft Microsoft geen directe invloed. Daarmee is sprake van feitelijke verwerkingsverantwoordelijkheid van de overheidsinstantie (de derde van de drie mogelijkheden geschetst in de vorige paragraaf) als het gaat om de verzending van telemetriegegevens aan Microsoft. Dat betekent dat daarvoor de overheidsinstantie eveneens verwerkingsverantwoordelijke is. Er is daarmee sprake van gezamenlijke verwerkingsverantwoordelijkheid als bedoeld in art. 26 AVG.

Voor de verwerking van verzamelde telemetriegegevens door Microsoft Corp. is uitsluitende Microsoft Corp. de verwerkingsverantwoordelijke. Dit geldt ook voor de verstrekking (lees: het via onder meer een beheerpaneel ter beschikking stellen) van die gegevens aan de overheidsinstantie. Voor de eventuele verwerking van de telemetriegegevens door de overheidsinstantie is alleen zijzelf verwerkingsverantwoordelijke.

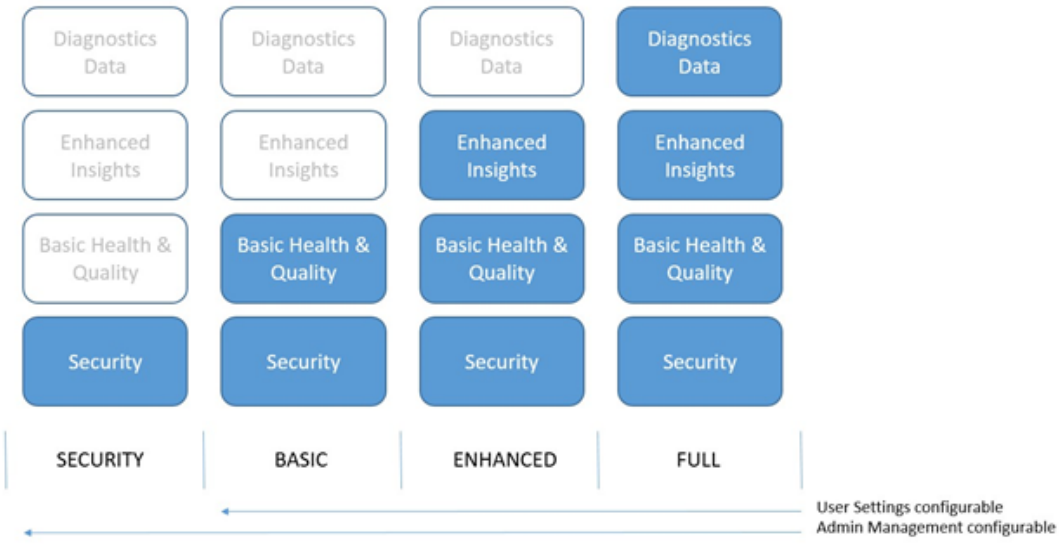
Microsoft heeft aangegeven het niet eens te zijn met bovenstaande zienswijze waar het de medeverantwoordelijkheid betreft van de overheidsinstantie:[72]

> Microsoft does not agree with the Ministry's assessment that we are a joint controller with our customers with respect to Windows 10 data processing. Microsoft is the independent and sole controller, and Microsoft determines the ways and means of processing. Enterprise customers are given substantial choice and control over the amount of data processed, but where that data is collected by Microsoft, it is wholly within Microsoft's control and responsibility to comply with controller obligations under the GDPR.

[72] Annex 2.

Bijlage 2 – Telemetrie in Windows 10

Microsoft verschaft op haar website uitgebreide informatie over de verwerking van telemetriegegevens en de invloed die de klant daarop kan uitoefenen. De basispagina is "Configure Windows diagnostic data in your organization".[73] In de linkermarge staan verwijzingen naar webpagina's waarin zeer gedetaillerd staat opgesomd welke gegevens er op de verschillende niveaus van telemetrie worden verwerkt.[74] Hieronder de minder gedetailleerde samenvatting die Microsoft geeft van de gegevensverwerking op de verschillende niveaus.



Niveau Security

- Connected **User Experiences and Telemetry component settings**. If general diagnostic data data has been gathered and is queued, it is sent to Microsoft. Along with this diagnostic data, the Connected User Experiences and Telemetry component may download a configuration settings file from Microsoft's servers. This file is used to configure the Connected User Experiences and Telemetry component itself. The data gathered by the client for this request includes OS information, device id (used to identify what specific device is requesting settings) and device class (for example, whether the device is server or desktop).
- **Malicious Software Removal Tool (MSRT)** The MSRT infection report contains information, including device info and IP address. (uitzetten heeft alleen invloed op MSRT)
- **Windows Defender/Endpoint Protection**. Windows Defender and System Center Endpoint Protection requires some information to function, including: anti-malware signatures,

[73] https://docs.microsoft.com/nl-nl/windows/configuration/configure-windows-diagnostic-data-in-your-organization.
[74] Zoals https://docs.microsoft.com/nl-nl/windows/configuration/basic-level-windows-diagnostic-events-and-fields voor niveau Basic.

diagnostic information, User Account Control settings, Unified Extensible Firmware Interface (UEFI) settings, and IP address. (uitzetten heeft alleen invloed op de app windows defender)

Niveau Basic

- **Basic device data**. Helps provide an understanding about the types of Windows devices and the configurations and types of native and virtualized Windows Server 2016 in the ecosystem. Examples include:
  - Device attributes, such as camera resolution and display type
  - Internet Explorer version
  - Battery attributes, such as capacity and type
  - Networking attributes, such as number of network adapters, speed of network adapters, mobile operator network, and IMEI number
  - Processor and memory attributes, such as number of cores, architecture, speed, memory size, and firmware
  - Virtualization attribute, such as Second Level Address Translation (SLAT) support and guest operating system
  - Operating system attributes, such as Windows edition and virtualization state
  - Storage attributes, such as number of drives, type, and size
- **Connected User Experiences and Telemetry component quality metrics**. Helps provide an understanding about how the Connected User Experiences and Telemetry component is functioning, including % of uploaded events, dropped events, and the last upload time.
- **Quality-related information**. Helps Microsoft develop a basic understanding of how a device and its operating system are performing. Some examples are the device characteristics of a Connected Standby device, the number of crashes or hangs, and application state change details, such as how much processor time and memory were used, and the total uptime for an app.
- **Compatibility data**. Helps provide an understanding about which apps are installed on a device or virtual machine and identifies potential compatibility problems.
  - **General app data and app data for Internet Explorer add-ons**. Includes a list of apps that are installed on a native or virtualized instance of the OS and whether these apps function correctly after an upgrade. This app data includes the app name, publisher, version, and basic details about which files have been blocked from usage.
  - **App usage data**. Includes how an app is used, including how long an app is used, when the app has focus, and when the app is started
  - **Internet Explorer add-ons**. Includes a list of Internet Explorer add-ons that are installed on a device and whether these apps will work after an upgrade.
  - **System data**. Helps provide an understanding about whether a device meets the minimum requirements to upgrade to the next version of the operating system. System information includes the amount of memory, as well as information about the processor and BIOS.
  - **Accessory device data**. Includes a list of accessory devices, such as printers or external storage devices, that are connected to Windows PCs and whether these devices will function after upgrading to a new version of the operating system.
  - **Driver data**. Includes specific driver usage that's meant to help figure out whether apps and devices will function after upgrading to a new version of the

operating system. This can help to determine blocking issues and then help Microsoft and our partners apply fixes and improvements.

- **Microsoft Store**. Provides information about how the Microsoft Store performs, including app downloads, installations, and updates. It also includes Microsoft Store launches, page views, suspend and resumes, and obtaining licenses.

Niveau Enhanced

- **Operating system events**. Helps to gain insights into different areas of the operating system, including networking, Hyper-V, Cortana, storage, file system, and other components.
- **Operating system app events**. A set of events resulting from Microsoft applications and management tools that were downloaded from the Store or pre-installed with Windows or Windows Server, including Server Manager, Photos, Mail, and Microsoft Edge.
- **Device-specific events**. Contains data about events that are specific to certain devices, such as Surface Hub and Microsoft HoloLens. For example, Microsoft HoloLens sends Holographic Processing Unit (HPU)-related events.
- **Some crash dump types**. All crash dump types, except for heap dumps and full dumps.

Niveau Full

Relevant als aangesloten (opted-in) voor het windows insider programma.

Alle gegevens van andere niveau's plus de mogelijkheid om met behulp van diagnostische tools extra informatie uit de systemen te krijgen

- Ability to run a limited, pre-approved list of Microsoft certified diagnostic tools, such as msinfo32.exe, powercfg.exe, and dxdiag.exe.
- Ability to get registry keys.
- All crash dump types, including heap dumps and full dumps.

Bijlage 3 – Telemetrie-instellingen voor Windows 10 Enterprise edition

1. Automatic Root Certificates Update
2. Cortana and Search
3. Date & Time
4. Device metadata retrieval
5. Find My Device
6. Font streaming
7. Insider Preview builds
8. Internet Explorer
9. Live Tiles
10. Mail synchronization
11. Microsoft Account
12. Microsoft Edge
13. Network Connection Status Indicator
14. Offline maps
15. OneDrive
16. Preinstalled apps
17. Settings > Privacy
    - 17.1 General
    - 17.2 Location
    - 17.3 Camera
    - 17.4 Microphone
    - 17.5 Notifications
    - 17.6 Speech, inking, & typing
    - 17.7 Account info
    - 17.8 Contacts
    - 17.9 Calendar
    - 17.10 Call history
    - 17.11 Email
    - 17.12 Messaging
    - 17.13 Phone calls
    - 17.14 Radios
    - 17.15 Other devices
    - 17.16 Feedback & diagnostics
    - 17.17 Background apps
    - 17.18 Motion
    - 17.19 Tasks
    - 17.20 App Diagnostics
18. Software Protection Platform
19. Storage Health
20. Sync your settings
21. Teredo
22. Wi-Fi Sense
23. Windows Defender
24. Windows Media Player
25. Windows Spotlight
26. Microsoft Store
    - 26.1 Apps for websites
27. Windows Update Delivery Optimization
28. Windows Update

Bijlage 4 – Relevante wetgeving VS

Het inschakelen van een buitenlandse leverancier van clouddiensten brengt het risico met zich mee dat de gegevens onder het recht van dat land kunnen worden opgevraagd door de lokale autoriteiten, zoals politie en justitie en inlichtingendiensten. Aldus vormt het buitenlandse recht een potentieel risico voor zowel de gegevens (security) als de betrokkenen (privacy), zeker als het betreffende land niet is onderworpen aan de Europese verdragen inzake privacy en bescherming van persoonsgegevens, met name het Europees Verdrag voor de Rechten van de Mens (EVRM) en het Handvest voor de Grondrechten van de Europese Unie (CFR).

Voor de Verenigde Staten zijn de volgende Amerikaanse wetten relevant:
- Foreign Intelligence Security Act (FISA)
- Stored Communications Act
- CLOUD Act
- Electronic Communications Privacy Act (ECPA)

Foreign Intelligence Security Act (FISA)

De FBI heeft de bevoegdheid om 'foreign intelligence information' van non-US persons die in het buitenland verblijven op te vragen bij Amerikaanse bedrijven (50 U.S. Code, paragraaf1881a, onderdeel van de Foreign Intelligence Security Act, FISA). *Foreign intelligence information* is een nogal brede term waarmee informatie die relevant is voor de nationale veiligheid van de VS is bedoeld. Deze bevoegdheid is opgenomen in de USA Freedom Act, de opvolger van de Patriot Act, die sinds 1 juni 2015 verlopen is. De USA Freedom Act vormt zowel een voortzetting als een beperking van de Patriot Act. De bevoegdheid om gegevens op te vragen is niet ongelimiteerd. De FBI moet daarvoor eerst toestemming krijgen van een speciale rechtbank, het FISA Court. De bevoegdheid om gegevens op te vragen lijkt zich echter niet uit te strekken tot gegevens die zich buiten de VS bevinden, zoals de servers van Microsoft in Ierland. De gegevens die door Microsoft Corp. worden verwerkt vallen wel onder de reikwijdte van de FISA.

Stored Communications Act

De Stored Communications Act (18 U.S. Code, Chapter 121 paragraaf 2701–2712) verplicht Amerikaanse bedrijven om gegevens te overhandigen aan de Amerikaanse Justitie (vergl. ons art. 126nd Wetboek van Strafvordering, waarin een vergelijkbare regel staat). Er loopt momenteel een gerechtelijke procedure in de Verenigde Staten over de vraag of de Amerikaanse Justitie op grond van de Stored Communications Act van Microsoft mag eisen dat persoonsgegevens die in Europa zijn opgeslagen aan de Amerikaanse Justitie worden overlegd in het kader van strafrechtelijk onderzoek. In een eerdere rechtszaak was Microsoft door een lagere federale rechter bevolen om gegevens die waren opgeslagen in haar datacenter in Ierland te overleggen onder het idee dat het ging om een Europese vestiging van een Amerikaans bedrijf en dat "dus" de Stored Communications Act op die data van toepassing is. Op 14 juli 2016 heeft het Amerikaanse Federale Gerechtshof (2nd Circuit) in hoger beroep bepaald dat de Stored Communications Act zich niet uitstrekt tot gegevens die in het buitenland zijn opgeslagen. M.a.w., Microsoft hoeft de gegevens in haar Europese cloud niet te overhandigen aan de Amerikaanse Justitie als deze daarom vraagt. De zaak ligt inmiddels bij het US Supreme Court die naar verwachting in de zomer van 2018 uitspraak zal doen.

CLOUD Act

De voornoemde zaak bij het US Supreme Court is grotendeels achterhaald door de recentelijk door het Congress aangenomen Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"), waarmee een verduidelijking van de in de Stored Communications Act bedoelde regels wordt bewerkstelligd als het gaat om gegevens die zich buiten de VS bevinden. De CLOUD Act is wel relevant voor de

gegevens van de Gebuiker die op Microsoft servers in Ierland zijn opgeslagen, maar niet voor de telemetriegegevens die door Microsoft Corp. worden verwerkt.

paragraaf 2713 van de CLOUD Act zegt het volgende:
''A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.''.

Paragraaf 2713 is van toepassing op de gegevens van "United States Persons". Hiermee worden onder ander niet alleen inwoners van de VS bedoeld, maar ook mensen met de Amerikaanse nationaliteit, ook als deze in Nederland wonen of verblijven (paragraaf 2523). Echter, paragraaf 2703 laat toe dat Microsoft verweer voert door aan te tonen dat de betreffende US Person niet in de VS woont. Wij zien alleen niet in hoe Microsoft dat zou kunnen vaststellen voor gegevens die door Nederlandse overheidsinstanties in de cloud van Microsoft Ierland worden opgeslagen. Derhalve zien wij dit niet als een effectieve beschermingsmaatregel. Aan de andere kant is het risico mogelijk laag, omdat er waarschijnlijk maar een beperkt aantal personen met een Amerikaanse nationaliteit bij Justitie & Veiligheid werken, waardoor de meeste medewerkers dus buiten de reikwijdte van de CLOUD Act vallen. Dit wordt anders als gegevens *over* US Persons door JenV met behulp van Office 365 worden verwerkt. Dat zijn er, mede gelet op de activiteiten in het JenV-domein, mogelijk veel meer en omvat mogelijk ook personen die wel in de VS wonen.

Een tweede beschermingsmaatregel is dat Microsoft aantoont dat het verstrekken van de gegevens in strijd is met lokale wetgeving (lees: de AVG en Iers recht). In dat kader wijzen wij op artikel 48 AVG, die Microsoft Ierland verbiedt om medewerking te verlenen aan het opvragen van gegevens onder de CLOUD Act als daar geen Mutual Legal Assistance Treaty (MLAT) of andere afspraak met de VS aan ten grondslag ligt.[75] In dat verband is de paragraaf over 'Executive Agreements' in de CLOUD Act relevant, waarmee de Amerikaanse overheid en de Ierse overheid overeen kunnen komen om gegevens op te vragen in elkaars jurisdictie. Maar linksom of rechtsom is de Nederlandse overheid niet betrokken bij een dergelijke afspraak of bij het toezicht daarop.[76]

Electronic Communications Privacy Act (ECPA)

De Electronic Communications Privacy Act (ECPA, 18 U.S. Code paragraaf 2510 e.v.) regelt onder welke voorwaarden de Amerikaanse Justitie data 'in transit' mag opvragen ('wiretapping'). Dit omvat dus ook het onderscheppen van de telemetriegegevens van en naar Microsoft Corp op het Amerikaanse deel van het netwerk.

---

[75] Art. 48 AVG: Elke rechterlijke uitspraak en elk besluit van een administratieve autoriteit van een derde land op grond waarvan een verwerkingsverantwoordelijke of een verwerker persoonsgegevens moet doorgeven of verstrekken, mag alleen op enigerlei wijze worden erkend of afdwingbaar zijn indien zij gebaseerd zijn op een internationale overeenkomst, zoals een verdrag inzake wederzijdse rechtsbijstand, tussen het verzoekende derde landen en de Unie of een lidstaat, onverminderd andere gronden voor doorgifte uit hoofde van dit hoofdstuk.

[76] In dit verband willen wij ook vermelden dat de Ierse Data Protection Commissioner in een (informeel) gesprek die wij met haar hadden over de positie van de Nederlandse overheid bij gebruik van cloud services in Ierland aangaf dat de Nederlandse overheid net als ieder ander een klacht bij haar mag indienen. Tenzij daar dus uitdrukkelijke afspraken over worden gemaakt met de Ierse toezichthouder, krijgt JenV dus geen voorkeursbehandeling bij de Ierse toezichthouder.

Bijlage 5 – Antwoorden van Microsoft

Annex 1: Deploying GDPR Compliant Windows 10 Enterprise and Office 365

Deploying Windows 10 Enterprise in compliance with GDPR

Windows 10 provides capabilities to help our Enterprise customers comply with the GDPR requirements to implement appropriate technical and organizational security measures to protect personal data. With Windows 10, the ability to protect, detect and defend against the types of attacks that can lead to data breaches is greatly improved. Enterprise customers have a number of configuration options for implementing Windows 10 using MDM and Group Policies to enable GDPR compliance. In this section, Microsoft describes the options and provides links to additional information available online.

Windows 10 Enterprise Creators Update (1703) & Fall Creators Update (1709)

Configuring the Windows 10 diagnostic settings

Windows diagnostic data is vital technical data from Windows devices about the device and how Windows and related software are performing. Diagnostic data can sometimes be confused with functional data. Some Windows components and apps connect to Microsoft services directly, but the data they exchange is not diagnostic data. Microsoft confirms that customers who set diagnostic data to Basic in the context of GDPR can do so with confidence.

Details on how to configure diagnostic settings can be found here [https://docs.microsoft.com/enus/windows/configuration/configure-windows-diagnostic-data-in-your-organization#enterprisemanagement].

Windows 10 Enterprise RS4

The spring 2018 release of Windows 10 Enterprise will offer enhancements to transparency and provide more automated tools to exercise data subject rights. These enhancements are as follows:

- **Delete by Device ID**

  For additional control over Windows diagnostic data processing, users can send an instruction from their Windows device to have the Windows diagnostic data associated with that device deleted from Microsoft's data stores. This user control can be found in Settings > Privacy > Feedback and Diagnostics.
- **Diagnostic Data Viewer**

  For additional transparency with Windows diagnostic data processing, users can use the Windows Diagnostic Data Viewer tool to view and search the data that is being collected from their device. Users can provide feedback to Microsoft on the content they see in the tool. More information on this tool can be found here Diagnostic Data Viewer Overview.
- These features will enable compliance with the GDPR for diagnostic data to be collected at any level. These Enterprise controls support Microsoft as Controller:
  - **Allow Telemetry:** This policy setting determines the amount of Windows diagnostic data collected by Microsoft.
  - ***New* Configure telemetry opt-in change notifications:** This policy setting determines whether a device shows notifications about telemetry levels to people on first

logon or when changes occur in Settings. Microsoft recommends enabling this control for Enterprises with employees in the EU.

- ***New* Configure telemetry opt-in setting user interface:** This policy setting determines whether users can change their own diagnostic levels in Settings and should be used in conjunction with the Allow Telemetry setting.

Additional tools to enhance control over data collection

Managing connections from Windows 10 components to Microsoft Services

Some Windows components, apps, and related services transfer data to Microsoft network endpoints. Details about the different ways to control traffic to these endpoints are described in Manage connections from Windows operating system components to Microsoft services. You can evaluate which other connections Windows makes to Microsoft services and determine whether or not to turn them off in your environment.

- The lowest connection configuration of Windows 10 Enterprise is the Windows Restricted Traffic Limited Functionality Baseline which is available for all versions of the Windows 10 operating system. This option disables all endpoints either using an automated script or manually. More information can be found online here [https://docs.microsoft.com/en-us/windows/configuration/manage-connections-from-windows-operating-system-componentsto-microsoft-services].
- Customers can individually manage connections from Windows operating system components to Microsoft services using the online documentation here [https://docs.microsoft.com/enus/windows/configuration/manage-connections-from-windows-operating-system-componentsto-microsoft-services].

Windows Telemetry Viewer

A similar tool to the Windows Diagnostic Data Viewer is available, under NDA, from the Microsoft Store. It is a simpler tool than the upcoming Diagnostic Data Viewer that only shows data collected at the Basic level of Windows Diagnostic Data collection for users on the Fall Creators Update (1709).

Deploying Office 365 E3/E5 (includes Office ProPlus) in compliance with GDPR

Office 365 Enterprise E3 and E5 plans consist of familiar Office applications (e.g., Outlook, Word, Excel) provided as Office 365 ProPlus client software, together with online services such as Exchange Online, OneDrive for Business, and Skype for Business, as more fully described on our website here.

Customers evaluating Office 365 from a GDPR perspective should first consider circumstances in which personal data will or may be processed in Office 365, related to both client software and online services.

The Office 365 ProPlus client software provides customers with user level controls for collection of personal data. Telemetry data can currently be controlled using a registry key; however, a separate user control will be available to customers in May. If an organizational customer does not wish to enable its users to use the small number of ProPlus connected online services for which Microsoft is a data controller (e.g., intelligent services powered by Bing such as translation) these services can be "toggled off" for the entire organization by the IT administrator.

The customer is accountable to decide which Office 365 Online Services are made available to its users (via assignment of licenses), to configure optional service features or capabilities in a manner the customer deems appropriate to meet their requirements, and to train users in use of the Online

Services in a manner consistent with laws or other requirements to which the customer is subject, not limited to GDPR.

To aid customers in evaluating the Online Services, extensive public documentation describes Office 365 service features and capabilities. See Office 365 Service Descriptions. Additionally, customers have available a wealth of compliance, security, and privacy information at the Microsoft Trust Center, and may review documentation that articulates both Microsoft and customer controls to meet GDPR and applicable 3rd party audit reports at the Service Trust Portal. Microsoft documents an approach that customers can take to managing their data using our cloud here: Office 365 Information Protection for GDPR. In advance of May, Microsoft will be releasing additional privacy information intended to assist customers in preparing their own Data Protection Impact Assessments where customers determine these are required.

Annex 2: Responses to Ministry of Justice and Security Questions

Microsoft received confirmation of the outstanding questions from the Ministry on February 28, 2018. This annex provides responses to these questions.

Windows Telemetry Questions

1. What is the roadmap for Windows portal capabilities being made available to enterprise and how does Microsoft audit/validate this?

   a. This question is unclear. We request that the Ministry identify which portal is being referenced.

2. What are the details on privacy impact assessments and what can Microsoft share to assist?

   a. Microsoft is preparing all of the Impact Assessments for its products and services required by the GDPR. Material information required by our commercial customers in order to prepare their own DPIAs will be shared through the Service Trust Portal prior to the enforcement of the GDPR.

3. What contractual commitments and other efforts does Microsoft offer to help with managing issues with customers (examples: communication to employees, privacy statements, lawful basis for processing, contractual relationship as employer and responsibilities as employees).

   a. The question about contractual commitments is addressed in the letter.
   b. The processing of Windows diagnostic data is described in the Microsoft Privacy Statement.
   c. Details of the mechanisms by which Data Subjects can exercise their Data Subject Rights will be included in the materials shared on the Service Trust Portal prior to the enforcement of the GDPR.
   d. Other Windows 10 Enterprise and Office 365 features coming in the spring 2019 release are described in Annex 1.

4. The Ministry of Justice (MoJ) believes that Microsoft and the MoJ are joint controllers in relation to the diagnostic and event data which Microsoft Corp collects via, amongst others, the Windows 10 telemetry functionality. Believe parties need to agree on "Arrangements" as specified in article 26.2. What is Microsoft's response to this?

   a. Microsoft does not agree with the Ministry's assessment that we are a joint controller with our customers with respect to Windows 10 data processing. Microsoft is the independent and sole controller, and Microsoft determines the ways and means of processing. Enterprise customers are given substantial choice and control over the amount of data processed, but where that data is collected by Microsoft, it is wholly within Microsoft's control and responsibility to comply with controller obligations under the GDPR.

5. The vortex endpoint v10.vortex.microsoft.com is used by optional programs such as Office to send telemetry. Will this kind of Telemetry be completely visible in the JSON files and the viewer tool? Can Microsoft provide information as to how this information which is currently not visible through the transparency tools be made visible to our security personnel? Which tools are required?
    a. The data viewable in the Data Viewer is the Windows diagnostic data collected from the machine on which the tool is running regardless of endpoint it is sent to. Windows diagnostic data is data controlled by the Diagnostic data setting. The tool does not show all the data that is sent to a given endpoint.
    b. Security features are in place to protect against 3rd party tampering with the data collected (such as certificate pinning and encryption of data in transit). There are no readily-available tools or mechanisms to see the detail of all the data that flows from Windows to Microsoft.
    c. For Office 365 ProPlus client software client application telemetry, Microsoft currently does not have a tool that is available. It would be possible to host the Ministry in the Transparency Centers and demonstrate the Office 365 ProPlus client software client application telemetry collection and explain the telemetry controls available.
    d. Office 365 ProPlus client application network traffic is over HTTPS, so 3rd party tools like Telerik's Fiddler can also be leveraged to analyze these data streams.

6. Can Microsoft provide documentation on what data is sent per optional program and how to manipulate the on/off function?
    a. Optional Microsoft services that run on Windows make network connections by default to collect data are described in the following online documentation: Manage Connections from Windows Operating System Components to Microsoft Services. This document describes briefly what each of these services do and how to turn each off. Additional detail about the data processed can be found in the Microsoft Privacy Statement.
7. If you run the Zero Emissions admx scripts will it also kill all telemetry caused by optional programs such as Office?
    a. The Zero Emissions admx script will discontinue Windows diagnostic data collection and data collection from the services described in Manage Connections from Windows Operating System Components to Microsoft Services. This includes apps that come preinstalled with some versions of Windows, including OneNote and the Get Office app, but does not disable any data collection from apps and services that are later installed by the customer.
    b. Office 365 ProPlus client software has several controls that can be utilized to disable certain data collection. These can also be controlled via Group Policy to provide an organization a scalable solution to apply these settings across their organization. Additionally, consumers will have an explicit consent experience starting in May to control things like telemetry.

8. Can Microsoft provide information relating to the minimum version of Windows 10 Enterprise required to apply Redstone 4?
    a. Customers can apply the Redstone 4 update to any version of Windows 10.

9. Microsoft stated that Microsoft would be a sole controller for all the [Windows] Telemetry related data. In that case we would like to review the Article 35 Data protection Impact assessment. Will Microsoft provide this information?
    a. With respect to Windows 10 Enterprise, we are in the process of completing customerfacing documentation which details the key aspects of GDPR compliance.

We do not have plans at this point to share our internal data protection impact assessments with customers but will ensure relevant materials needed to help customers complete their own impact assessments are made available to them prior to the enforcement of the GDPR.

10. Microsoft is using multiple legal entities in various countries outside and inside the EU as a controller to deliver its services therefore Binding Corporate Rules are required. Can Microsoft provide a copy of the approved BCR's? If not yet approved, please explain status.
    a. Microsoft complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States. Microsoft has also implemented the standard contractual clauses for data transfers.

11. Microsoft advised that the Telemetry setting "basic" plus some extra setting was recommended to maintain functionality including Windows ATA type functionality. Can Microsoft specify exactly which switches need to be ON to achieve this?
    a. This question is unclear. Is the Ministry asking about Windows Advanced Threat Protection (ATP) or Windows Analytics?

12. Microsoft will deliver a telemetry OFF mode through a script for administrators – this is called 'ZeroEmissions' – with which all data streams from Windows 10 to Microsoft can be switched off. Turning of these data streams however has several disadvantages, because in doing this, desired security features that are required for malware detection and treat analysis, will be switched off as well. Because of this, Windows products will be less functional and additional software products from third parties have to be brought in to restore the security functionality. Apart from the fact that applying the ZeroEmissions script will lead to a disinvestment in the purchased Microsoft technology, it will increase the managing costs significantly and it will obstruct future innovation. Microsoft's advice is to not switch off the telemetry, but to set it to a
    "Basic" level and to add some data elements that are required for the security related functionality. Please confirm if this is correct.
    a. Collecting data at the Basic diagnostic level enables Microsoft to get information we need to help keep devices up-to-date and secure.
    b. The Security diagnostic level is an option for Enterprises, but they will need to do more to manage the compatibility and success of their own Windows Updates. Turning off Windows Defender and the Malicious Software Removal Tool (MSRT) is also possible to minimize data flows, but we do not recommend that unless the company replaces these functions with an alternative antimalware solution.
    c. The Zero Emissions script turns the diagnostic level to Security, and turns off Windows
       Defender and MSRT and all the data flows described in Manage Connections from Windows Operating System Components to Microsoft Services. The consequences of turning off those data flows are generally described in that document.
    d. You can learn more about how to configure Windows to use Windows Defender Advanced Threat Protection in windows-defender-advanced-threat-protection which covers data storage and privacy.
    e. You can also learn more about how to configure Windows to use Windows Analytics in upgrade-readiness-get-started, which covers data collection and privacy.

13. Microsoft will add a button to Windows Enterprise that can remove all telemetry that is stored with Microsoft in the United States when and if the user activates this button. The user must periodically activate this button himself/herself.
    - Information gathered by Windows 10 will be made visible per PC through a file in JSON format that will be visible for the user through a data viewer tool.
    - Windows 10 security and privacy settings will be redesigned, as a result of which there will be more settings in Windows 10. However, overall it will look more organized for the user.
    - At a later stage, there will be a centralized possibility to centrally evaluate the JSON files from all PCs in an organization.

    Please c onfirm if this is correct.

    a. Microsoft is adding a device-based Windows diagnostic data delete control to the Diagnostics & Feedback Setting page in RS4 for all editions of Windows 10 (not solely Enterprise). This button allows the user to delete all the Windows Diagnostic Data that Microsoft has collected which is still associated with the deviceID of the device.

    b. The capability to centrally view Windows Diagnostic Data collected from multiple devices in an organization is being discussed internally, and with customers to gather feedback and determine whether it might be prioritized for delivery at some future date.

    c.

14. We understand that a profile is kept on a per user basis at Microsoft which is compiled by combining various data sources. Can Microsoft please explain how this works in detail taking into account that the corporate username email combination often is also the Microsoft Live ID.

    Is there a DPIA available at Microsoft for this profile and the associated processes?

    a. This question is unclear. Please provide more information.

Bijlage 6 – Referenties

De genoemde op internet toegankelijke documenten zijn geraadpleegd op of omstreeks 26 april 2018.

https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization

https://docs.microsoft.com/en-us/windows/configuration/manage-connections-from-windows-operating-system-components-to-microsoft-services.

https://docs.microsoft.com/en-us/windows/deployment/update/windows-analytics-overview.

https://privacy.microsoft.com/nl-NL/privacystatement

https://docs.microsoft.com/en-us/windows/configuration/configure-windows-diagnostic-data-in-your-organization#understanding-windows-diagnostic-data

https://tools.ietf.org/html/draft-ietf-websec-key-pinning-21

https://blogs.windows.com/windowsexperience/2018/01/24/microsoft-introduces-new-privacy-tools-ahead-of-data-privacy-day/

Artikel 7:611 Burgerlijk Wetboek.

G.J.J. Heerma Van Voss¸ Goed werkgeverschap als bron van vernieuwing van het arbeidsrecht, 1993, p. 85.

ECLI:NL:RBAMS:2018:1644. “4.8. In het verweer van Google ligt mede besloten dat zij zich erop beroept dat artikel 16 Wbp, waarmee de Privacy Richtlijn is geïmplementeerd, niet dient te gelden in het geval van het beschikbaar maken voor het publiek door een zoekmachine van publicaties waarin wordt bericht over strafrechtelijke persoonsgegevens betreffende medeburgers.

Advies 1/2010 over de begrippen “voor de verwerking verantwoordelijke” en “verwerker”, 16 februari 2010, 00264/10/NL, WP169.

advies van de Artikel 29 Werkgroep inzake Society for Worldwide Interbank Financial Telecommunication (SWIFT), 22 november 2006 (WP 128).

https://docs.microsoft.com/nl-nl/windows/configuration/basic-level-windows-diagnostic-events-and-fields voor niveau Basic.

Bijlage 7 – Lijst van begrippen

Artikel 29 Werkgroep De Artikel 29-werkgroep is het onafhankelijke advies -en overlegorgaan van Europese privacytoezichthouders. De werkgroep speelt een belangrijke rol in de totstandkoming van Europees beleid voor de bescherming van persoonsgegevens.

telemetriegegevens q Microsoft verzamelt voortdurend technische prestatie- en gebruiksgegevens over elk apparaat waarop Windows 10 is geïnstalleerd. Deze gegevens worden telemetriegegevens genoemd.

diagnostische gegevens Het lijkt erop dat "telemetrie" door Microsoft gedefinieerd wordt als de verwerking van diagnostische data. In het vervolg zullen we de termen "diagnostische gegevens" en "telemetriegegevens" door elkaar heen gebruiken.

event data ook wel systeemevents, een event is een actie of gebeurtenis die wordt herkend door software, vaak asynchroon afkomstig van de externe omgeving, die mogelijk door de software wordt verwerkt.

functionele gegevens inhoud van gebruikersbestanden

gebruikersgegevensq zie functionele gegevens

verwerkingsverantwoordelijke een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;

verwerker een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;

VOD *Voorwaarden voor Online Diensten*

Bijlage 8 – Afkortingen

AVG Algemene Verordening Gegevensbescherming

BIR Baseline Informatiebeveiliging Rijksdienst

BW Burgerlijk wetboek

BZK Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

CIO Chief Information Officer

CIP Centrum voor Informatiebeveiliging en Privacybescherming

ePV e-Privacyverordening

EVRM Europees Verdrag voor de Rechten van de Mens

FG Functionaris voor de Gegevensbescherming

GEB Gegevensbeschermingseffectbeoordeling

IMEI nummer, International Mobile Equipment Identity, IMEI staat voor het (meestal 15-cijferige) nummer dat een mobiel device identificeert

JenV Ministerie van Veiligheid en Justitie

MBSA Microsoft Business and Services Agreement

MSRT Malicious Software Removal Tool, Windows-hulpprogramma voor het verwijderen van schadelijke software

MvT Memorie van Toelichting

NEN/ISO Nederlands Normalisatie-instituut/ Internationale Organisatie voor Standaardisatie

Opt-in/out Opting, keuze mogelijkheid

PIA Privacy Impact Assessment

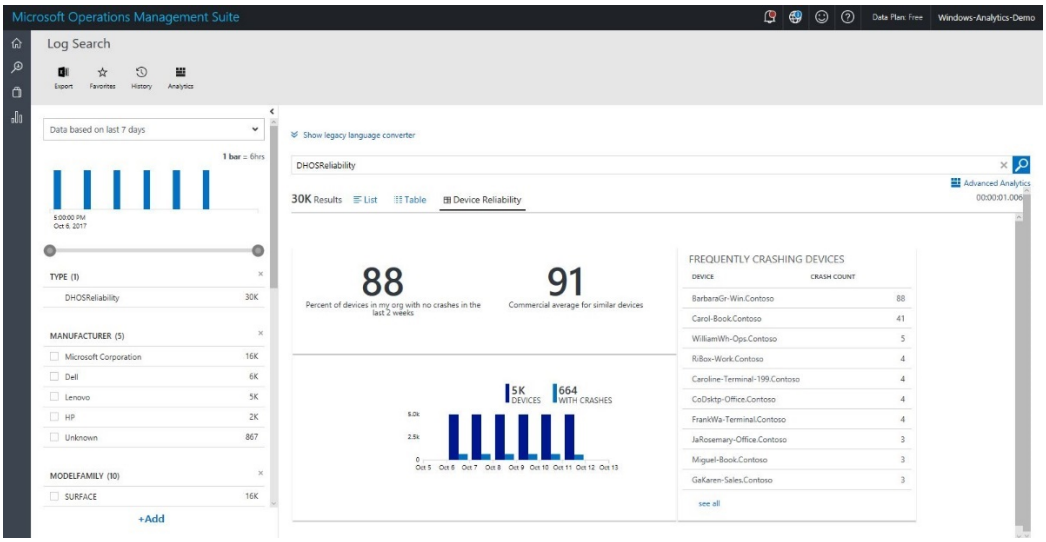
SLM Rijk Strategisch Leveranciersmanagement Rijksoverheid

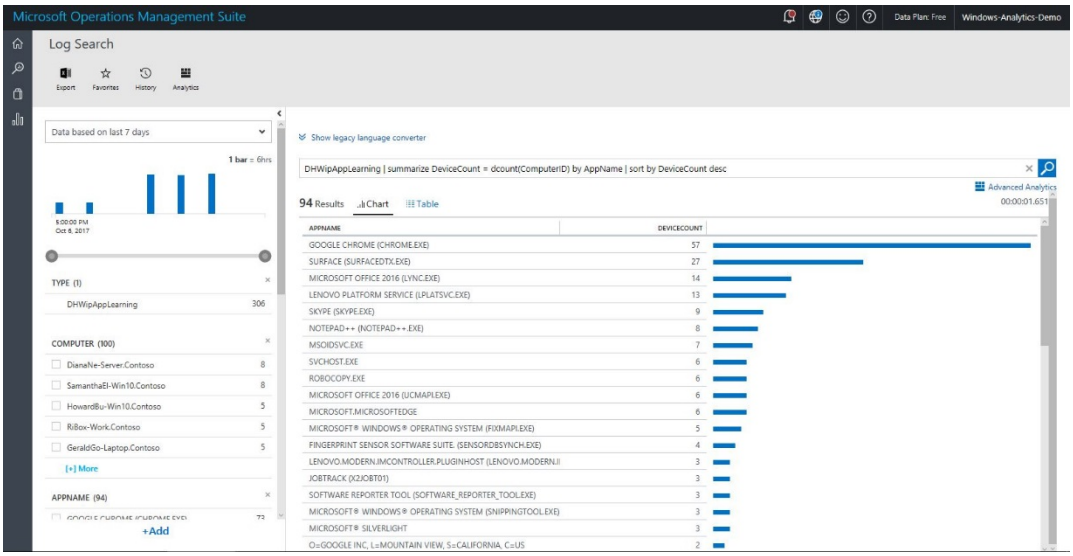
Tw Telecommunicatiewet

Wbp Wet bescherming persoonsgegevens

WSUS Windows Server Update Services, Met WSUS kunnen beheerders de distributie van updates die worden uitgegeven via Microsoft Update op de computers in het netwerk volledig beheren.

Bijlage 9 – Voorbeelden “Windows Analytics Device Health rapporten”






Maatregelen
nemen
Privacybewustwording
Doelbinding
PIA
Noodzaak
Effecten in kaart
Bescherming van
persoonsgegevens
Risico's
minimaliseren
Richtinggevend
Rechtsgrond
Met open vizier